NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

QUANTUM COMPUTATION

by
Dimitrios Giannakopoulos

June 1999

Thesis Advisor: James Luscombe
Second Reader: R. L. Armstead

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1999	Master's Thesis

4. TITLE AND SUBTITLE
QUANTUM COMPUTATION

5. FUNDING NUMBERS

6. AUTHOR(S)
Giannakopoulos Dimitrios

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Two seemingly unrelated scientific disciplines, information processing and quantum mechanics, were separately developed, until physicist Richard Feynman proposed their combination. Today, quantum computation is at the forefront of research in theoretical physics and computer science. The objectives of this thesis are to present an introduction to the subject of quantum computation and its potential, and to analyze the physics underlying the operation of one of the proposed realizations of a quantum logic gate, based on cavity quantum electrodynamics (QED). We discuss the fundamental aspects of quantum mechanics that may be a revolutionary new way to process information. We then present the appropriate theoretical background of QED needed to understand the proposed realization of a quantum gate. We identify the advantages and disadvantages of this realization. We then address and discuss the phenomenon of decoherence, the most fundamental obstacle to overcome for the development of practical quantum computers. Finally, some of the possible military applications are presented, along with our thoughts for the future of this field. We conclude that quantum gates based on cavity QED are feasible with current technology. However, the construction of a quantum network with these gates is not feasible, mainly due to the decoherence problems.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Quantum computing,cavity QED	97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

QUANTUM COMPUTATION

Dimitrios Giannakopoulos
Captain, Hellenic Air Force
B.S., Hellenic Air Force Academy, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN PHYSICS

from the

NAVAL POSTGRADUATE SCHOOL
June 1999

Author: _____
Dimitrios Giannakopoulos

Approved by: _____
James Luscombe, Thesis Advisor

_____
R.L. Armstead, Second Reader

_____
William Maier, Chairman
Department of Physics

ABSTRACT

Two seemingly unrelated scientific disciplines, information processing and quantum mechanics, were separately developed, until physicist Richard Feynman proposed their combination. Today, quantum computation is at the forefront of research in theoretical physics and computer science.

The objectives of this thesis are to present an introduction to the subject of quantum computation and its potential, and to analyze the physics underlying the operation of one of the proposed realizations of a quantum logic gate, based on cavity quantum electrodynamics (QED). We discuss the fundamental aspects of quantum mechanics that may be a revolutionary new way to process information. We then present the appropriate theoretical background of QED needed to understand the proposed realization of a quantum gate. We identify the advantages and disadvantages of this realization. We then address and discuss the phenomenon of decoherence, the most fundamental obstacle to overcome for the development of practical quantum computers. Finally, some of the possible military applications are presented, along with our thoughts for the future of this field.

We conclude that quantum gates based on cavity QED are feasible with current technology. However, the construction of a quantum network with these gates is not feasible, mainly due to the decoherence problems.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I feel that one of the most exciting parts of finishing a thesis is the opportunity to thank those who made it possible.

First of all I would like to thank the Hellenic Air Force for giving me the chance to attend NPS. Also, I would like to thank my professors of Department of Physics at NPS and especially my thesis advisor Dr. James Luscombe. I owe a great intellectual debt to him. Our conversations about various subjects gave me an insight and helped me learn a correct way of thinking physics. I feel obliged to Dr. Wolfgang Baer for his comments and ideas on the subject. Also I thank Dr. Andrés Larraza for his comments on QED theory and his effort to help me understand some of the difficult concepts involved.

I am also grateful to my parents that made the ultimate goal of their life to provide me with the best education and gave me the moral standards that helped me in every aspect of my life.

Finally, I think that I can never find words to express my deep gratitude to my lovely wife Vicki. She made sure all these years that I could work undisturbed and even gave me strength and inspiration when I needed it.

I. INTRODUCTION

Every two years for the past fifty, computers have become twice as fast while their components have become twice as small. The main reasons for this progress are the technological advances made in lithographic manufacturing techniques. The implementation of these techniques allows us to build sub-micron wide logic gates and wires, cramming them onto the surface of silicon chips. However, integrated circuit technology is running up against fundamental limits, due to the laws of physics. Even if we find new ways to manufacture smaller chips, ultimately they will be so small that they will be made out of a few atoms. Reaching the atomic scale, chip manufacturers will face the rules of quantum mechanics, which are quite different from the classical rules that determine the properties of today's conventional logic gates. So if computers are to become smaller in the future, it is inevitable that quantum mechanics will play an important role.

The point is, however, that quantum theory can offer not only the means for new technological breakthroughs in construction techniques, but it can support an entirely new kind of computation, the so-called quantum computation. On the other hand, the combination of quantum mechanics and computer theory can offer a new way of understanding quantum systems themselves.

That was the starting point for this new theory, as the physicist Richard Feynman proposed in 1982 a scheme for the simulation of quantum-mechanical

systems by other quantum systems, built for this purpose.[1,2] The next step that revealed the power of quantum computation was in 1985 when David Deutsch of the University of Oxford published a theoretical paper[3] in which he described a universal quantum computer and its potential. Simultaneously Deutsch and other physicists realized that quantum mechanics offered a way of overcoming one of the most fundamental difficulties of computer science, that of a unique computational complexity for every mathematical problem.[4] It was believed until then that the time needed to solve any given problem that was polynomial or greater in the size of its inputs was independent of the physical apparatus used to perform the computations. This axiom seems not to be true for quantum computers. It was this realization that made scientists all over the world start looking at the development of these new ideas.

For more than a decade after the first proposal the obstacles encountered were so many and difficult that it seemed this new theory would be yet another academic curiosity, without ever offering any of the initial believed benefits.

But in 1994, Peter Shor from AT&T's Bell Laboratories in New Jersey devised the first quantum algorithm that, in principle, could perform efficient factorization[5], something useful that only a quantum computer could do. Today, most of the methods used for encryption are based on the difficulty of factorization, thus allowing the privacy and security in our electronic transactions (bank accounts, credit cards, etc.). The fact that a quantum algorithm could solve this problem gave a new boost for the prospects of quantum computation.

Since then a growing number of scientists and institutes all over the world have developed various projects trying to explore the theoretical background and the technology needed to build a quantum computer.

In this thesis, first we analyze the elements of quantum mechanics that give a new way to process information and compare it wherever applicable with classical computational methods. Then we will briefly discuss some of the proposed realizations and applications for quantum computers. From these proposals we will focus on the one that uses the principles of cavity quantum electrodynamics to build the necessary quantum logic gates. We will review in Chapter IV the theoretical background needed for the implementation of these techniques. Then in Chapter V we will report some of the recent experiments based on cavity quantum electrodynamic techniques and we will describe a proposed 2-bit quantum universal gate. In Chapter VI we will discuss the most difficult obstacle needed to overcome for building a quantum computer, the phenomenon of decoherence. Finally in Chapter VII we present some possible military applications, while in Chapter VIII we discuss the possibility of building a quantum computer in the near future.

It should be noted that quantum computation is a part of a new evolving science called quantum information, which also includes quantum teleportation and quantum cryptography. Even though some of the aspects of the other two fields can be combined with quantum computation or can be used to solve some of the encountered problems, it is beyond the scope of this thesis to provide a

review or analysis for these fields. In some cases there may be a review of the advancements in these theories, which provide a deeper understanding of some of the aspects of quantum computation.

II. ELEMENTS OF QUANTUM COMPUTERS

Quantum computers are different from conventional ones due to their distinguished fundamental elements and their rather peculiar properties, which arise from quantum theory.

The most important elements of quantum mechanics that give these properties to quantum computers are the superposition of states, quantum entanglement, reversible unitary evolution, and decoherence. We will review these and explain their effects in the construction of a quantum machine. A quantum computer is made by quantum logic gates, which operate with quantum bits. The gates are connected with quantum "wires".

A. QUANTUM BITS AND REGISTERS

1. Definitions and Properties of Qubits and Registers

The quantum bit or simply called "qubit" is the building block of quantum logic, like the bit, which is the building block of conventional logic. Any quantum system that can have two accessible states can be used, at least theoretically, as a qubit. However, the property of superposition distinguishes a qubit from a classical bit. A classical bit can have only two choices 0 or 1 and is always in either of these states. The qubit, however can have an infinite number of superimposed states between the assigned values of 0 and 1. Its properties are based on these infinite states. Using mathematical terms we can say that the state of a quantum system is a vector in Hilbert space that can be written as a

superposition of basis vectors, chosen by us with certain mathematical properties.[6] For a two-state system in which we choose as basis vectors the classical realization for the states 0 and 1 we can write:

$$|\psi\rangle = a|0\rangle + b|1\rangle \qquad (1)$$

where a and b are normalized complex coefficients. Due to this definition the value of the qubit is uncertain. The probability to find the qubit in state 0 or in state 1 is given by $|a|^2$ or $|b|^2$ respectively. It should be noted here, that according to quantum theory, the measurement problem of a quantum system imposes a limitation on the accessible amount of information. Most of the information included in the superimposed states is not accessible to us, but it is nevertheless needed in order to predict the evolution of the system until its final state, which includes the solution.[7]

Since the qubit has a basis of two states we can infer that n qubits will have a basis of 2^n states. The collection of n qubits is called a quantum register in direct analog with a classical computer register, which is a collection of n bits. A classical register has one definite value even though it involves n bits. However, a quantum register consisting of n qubits can exist in a superposition of all possible classical states, thus allowing the performance of a single computation to solve a problem with many different inputs. This property is called quantum parallelism and gives the advantage of solving a problem in less time by utilizing a quantum machine.[8]

2. Entanglement

The notion of superposition for the n qubit register described before was very simple and did not include a fundamental property of quantum theory, called quantum entanglement.

Since 1935 when Einstein, Podolsky, and Rosen presented the famous EPR paradox[9], an endless debate has started considering entangled particles and their properties.

Schrödinger first used the term entanglement in one of his papers[10] in 1935, where he commented on the EPR paradox.[8] Two equivalent definitions for entanglement[6,11] are:

The states of the subsystems constituting a complete quantum system do not determine the state of the system.

Some definite states of a complete quantum system do not correspond to definite states of the subsystems.

We will try to describe entanglement for a system consisting of two subsystems[6,8]. Each subsystem has its own Hilbert space denoted by H_A and H_B. We assume that the vectors $|n\rangle_A$ and $|m\rangle_B$ are a complete orthonormal basis for the Hilbert spaces H_A and H_B respectively (with n,m=0,1,2,..). The total Hilbert space for the complete system is given by the tensor product of the individual Hilbert spaces of each subsystem, $H_A \otimes H_B$ or $|n\rangle_A \otimes |m\rangle_B \equiv |n\rangle_A |m\rangle_B$. So now we can write any state of the complete system as:

$$|\Psi\rangle_{AB} = \sum_{n,m} c_{nm} |n\rangle_A |m\rangle_B \qquad (2)$$

where c_{nm} are normalized complex coefficients with $\sum_{n,m} |c_{nm}|^2 = 1$. Now we define the direct product state as a state $|\Psi\rangle_{AB}$ of the complete system that can be factored as a tensor product of two normalized states $|\psi\rangle_A = \sum_n c_n |n\rangle_A$ and $|\psi\rangle_B = \sum_m c_m |m\rangle_B$:

$$|\Psi\rangle_{AB} = |\psi\rangle_A |\psi\rangle_B \qquad (3)$$

We can see that there are states in the Hilbert space $H_A \otimes H_B$ that are not direct product states. These are called entangled states. An example is the state $|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B$.

The property of entanglement is encountered in every aspect of quantum information theory and has been used in many applications such as quantum coding, quantum compression of information and quantum teleportation.

B. QUANTUM GATES

Logic gates perform information processing in a classical computer. The logic gates change the input bit in accordance with a truth table, defined by binary logic.

The quantum gate is implemented by means of a unitary evolution operator that changes the input state in accordance with the same truth table as in classical gates.[8,12]

Classical gates perform operations on definite states and have definite outputs, while quantum gates can perform operations in a superposition of input states resulting in a superposition of output states. This is the notion of quantum parallelism described before.

The key feature that makes quantum gates powerful is the unitary evolution, which ensures the isolated performance of operations and their reversibility. However, this feature is the most difficult obstacle to overcome in the implementation of quantum computing, since it is not easy to prepare a quantum system and make it evolve without any interference from the environment. This difficulty will be discussed in more detail later. Now we will analyze the notion of this unitary evolution operator and its correspondence with a quantum gate.

1. Reversible Unitary Evolution Operator

By definition[6] an operator U is unitary if its inverse U^{-1} is equal to its adjoint U^{+}, i.e. $U^{+}U=UU^{+}=I$. If H is a Hermitian operator then the operator $U=e^{iH}$ is unitary.

An isolated quantum system evolves in a reversible manner, according to the time dependent Schrödinger equation:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle \qquad (4)$$

Since equation (4) is linear and homogeneous we can infer that the correspondence between two states at different times is linear. Therefore we can

introduce a linear operator U(t, t_0), which evolves a state at time t_0 to a state at a later time t:

$$|\psi(t)\rangle = U(t,t_0)|\psi(t_0)\rangle \tag{5}$$

If we substitute (5) into (4) we have:

$$i\hbar\frac{\partial}{\partial t}U(t,t_0)|\psi(t_0)\rangle = H(t)U(t,t_0)|\psi(t_0)\rangle \Rightarrow i\hbar\frac{\partial}{\partial t}U(t,t_0) = H(t)U(t,t_0) \tag{6}$$

When the operator H does not depend on time we can obtain by integration of equation (6):

$$U(t,t_0) = e^{-iH(t-t_0)/\hbar} \tag{7}$$

and so the state at a time t can be written:

$$|\psi(t)\rangle = e^{-iH(t-t_0)/\hbar}|\psi(t_0)\rangle \tag{8}$$

The operator U is unitary and a quantum gate will perform calculations according to this operator, thus transforming the input state at time t_0 to an output state at time t. The operator H is the Hamiltonian of the closed quantum system. It does not involve any effects from the environment. It is now clear the reason why the system must be closed. Also it must be noted that while the computation is performed we can never know the states the gate runs through until we make the measurement at a time t. This has the consequence that a computation can be performed by many different ways, even though we always achieve the same final result[7].

Another fine point involving the unitary evolution operator is the dependence or not of the Hamiltonian H on time. Above we assumed that H was independent of time and we derived equation (8) for the evolution of the system. However, this is not the case when H depends on time. A lot of books discussing quantum computing define the evolution operator in this case as:

$$U(t,t_0) = e^{-\frac{i}{\hbar}\int_{t_0}^{t} H(t')dt'}$$

which is not always true[6]. The derivative of an operator of the form $e^{F(t)}$ is equal to $F'(t)e^{F(t)}$ only when F(t) and F'(t) commute. So if someone chooses to implement a quantum gate with a system described by a time dependent Hamiltonian, they must ensure the above commutation. When the Hamiltonian does not commute with itself at different times, the time evolution operator may be defined in terms of the Dyson time-ordering operator.[13]

The evolution of a closed quantum system described by a unitary operator provides us the theoretical background for the operation of a quantum logic gate. A system with two accessible states can be used, at least theoretically, to implement such a gate.[4] Many two state systems are known in physics. An example is the spin up and spin down states of a spin-1/2 elementary particle.

2. Density Operator

It often occurs that the state of a system is not perfectly determined or where a large number of identical quantum systems are used for the

implementation of a quantum gate. In these cases the evolution of the system can not be described by the unitary operator defined in the previous paragraph. However, there is a mathematical tool called the density operator, which ensures the simultaneous application of quantum mechanics and probability theory. The density operator is an alternative way to describe any quantum system. It also provides the basis for understanding the irreversibility problems involved in the evolution of quantum systems.[8] We first introduce the notion of density operator for a system whose state is perfectly known. This is called the pure state.[6] Then we will expand the definition for the non-pure case, where we have a statistical mixture of states.[6] It must be noted that in our treatment of various elements of quantum mechanics we will use the Dirac notation.

a) Density Operator in the Pure Case[6]

We consider a system with state vector:

$$|\psi(t)\rangle = \sum_n c_n(t)|u_n\rangle \tag{9}$$

where $|u_n\rangle$ are a complete set of orthonormal vectors in Hilbert space and the coefficients satisfy the relationship:

$$\sum_n |c_n(t)|^2 = 1 \tag{10}$$

The matrix elements of an observable A can be written as:

$$\langle u_n|A|u_m\rangle = A_{nm} \tag{11}$$

and its mean value is given by:

$$\langle A(t)\rangle = \langle \psi(t)|A|\psi(t)\rangle = \sum_{n,m} c_n^*(t)c_m(t)A_{nm} \qquad (12)$$

Equation (12) shows us that mean values of observables are given as quadratic expressions of $c_n^*(t)c_m(t)$. But from the definition of the state vector we can write:

$$c_n^*(t)c_m(t) = \langle u_m|\psi(t)\rangle\langle\psi(t)|u_n\rangle \qquad (13)$$

Now we define the density operator $\rho(t)$ as:

$$\rho(t) = |\psi(t)\rangle\langle\psi(t)| \qquad (14)$$

This can also be represented by a matrix called the density matrix, with elements:

$$\rho_{mn}(t) = \langle u_m|\rho(t)|u_n\rangle = c_n^*(t)c_m(t) \qquad (15)$$

Now that we have defined the operator we can find how a quantum state of the system is characterized. Using equation (15) equation (10) becomes:

$$\sum_n |c_n(t)|^2 = \sum_n \rho_{nn}(t) = Tr\rho(t) = 1 \qquad (16)$$

where $Tr[\rho(t)]$ is the trace of the matrix.

Using equations (11) and (15) equation (12) becomes:

$$\langle A(t)\rangle = \sum_{n,m}\langle u_m|\rho(t)|u_n\rangle\langle u_n|A|u_m\rangle = \sum_m \langle u_m|\rho(t)A|u_m\rangle = Tr[\rho(t)A] \qquad (17)$$

Finally if we use Schrödinger's equation we can write the evolution of the operator as:

$$i\hbar\frac{d}{dt}\rho(t) = [H(t), \rho(t)] \qquad (18)$$

The density operator is hermitian and for a pure state it satisfies:

$$\rho^2(t) = \rho(t),\ Tr\rho^2(t) = 1. \tag{19}$$

The last two relations are true only for the pure case.

b) *Density Operator for a Statistical Mixture of States (Non-Pure Case)*[6]

Now we consider a system whose state is not perfectly known. In this case we assign to each probable state of the system $|\psi_k\rangle$ a probability p_k, with $\sum_k p_k = 1$.

We define the density operator for the state $|\psi_k\rangle$ as $\rho_k = |\psi_k\rangle\langle\psi_k|$. Then the density operator at any time t is:

$$\rho(t) = \sum_k p_k \rho_k(t) \tag{20}$$

The trace of this operator is:

$$Tr\rho = \sum_k p_k Tr\rho_k = \sum_k p_k = 1 \tag{21}$$

The evolution of the operator is again given by equation (18) above. It is noted that the last two relations in (19) do not hold and we have:

$$\rho^2 \neq \rho,\ Tr\rho^2 \leq 1 \tag{22}$$

The density operator and its properties will be used in Chapter VI when the phenomenon of decoherence will be presented.

3. Universal Quantum Gates

As noted earlier one of the most important features of quantum gates is their reversibility. David Deutsch has defined[14] the universal quantum logic gate as the gate that can be used to simulate any quantum gate. Since early 1980s a lot of proposals have been published for such gates. It has also been shown that for classical reversible computation the simplest universal gate has three inputs and three outputs. From all the proposed schemes two gates have received the most attention as potential candidates for implementation in quantum computing, the Toffoli[15] and Fredkin[16] gate.

In the Toffoli gate two input bits control the state of the third bit (target). The control bits do not change between input and output. The state of the target bit changes when the two control bits are set to 1.

In the Fredkin gate there is one control bit and two target bits. The control bit does not change. The target bits swap states only when the control bit is set to 1. Tables 1 and 2 are the truth tables for the Toffoli and Fredkin gates, respectively.

INPUT BITS			OUTPUT BITS		
A(control)	B(control)	C(target)	A(control)	B(control)	C(target)
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1
0	0	1	0	0	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

Table 2.1 Toffoli gate

INPUT BITS			OUTPUT BITS		
A(target)	B(target)	C(control)	A(target)	B(target)	C(control)
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	0
0	0	1	0	0	1
0	1	1	1	0	1
1	0	1	0	1	1
1	1	1	1	1	1

Table 2.2 Fredkin gate

Even though a variety of systems have been proposed for the implementation of quantum computation only a few of them can exhibit their usage as a universal quantum gate. The difficulty of implementing systems with three bits has been reduced since 1995, when a team of scientists (Tycho Sleator and Harald Weinfurter) described a 2-bit universal quantum gate.[17] A 2-bit gate can be used as the building block for any quantum logic network. This was shown at the same time by other researchers as well (i.e. David di Vincenzo). The proposed scheme for the implementation of this gate is based on cavity quantum electrodynamics theory and specifically to the interaction of atoms with single mode fields of microcavities.

We have not yet mentioned a way for connecting the quantum gates. The so-called quantum wires are an important part for the construction of a quantum computer. Some proposals exist for such wires[4], but we are not going to describe any of them in this thesis.

III. PROPOSED APPLICATIONS AND REALIZATIONS FOR QUANTUM COMPUTERS

We present in this chapter some of the proposed applications for quantum computers. We also present a brief description of the basic proposed schemes for the implementation of quantum computers. Since the power of quantum computing is now starting to be revealed there will surely be more proposed applications in the future. Some of our thoughts for possible military applications will be presented later.

A. APPLICATIONS

Current conventional machines are capable of performing very complex computations and solving many difficult problems. However, there are some problems that either appear to be intractable or the time and computing power needed for the solution is enormous. Thus, most of the researchers in the field focused their efforts in quantum computers that could solve these special problems.

1. Factorization

As was noted earlier the difficulty of factoring large numbers is the key issue for efficient cryptography. Even though the factorization of a large integer cannot be considered classically intractable, it is very difficult since it requires huge computing power and a very large number of calculations. This is due to the insufficient classical algorithms for the solution of the problem.

In 1994 Peter Shor from AT&T's Bell Laboratories in New Jersey devised the first quantum algorithm that, in principle, could perform efficient factorization of large numbers.[5] This event was a major breakthrough and the factorization problem became one of the most interesting applications for quantum computers.

Shor's algorithm is based on the fact that factoring a number can be related to the problem of evaluating the period of a function.[8] Then the factors of the number can be found using number theory. The evaluation of a period of a function by classical computers is very difficult, since it requires the same computational power as the factorization problem. Quantum computers can solve this problem rather easily by using their advantage to perform the required calculations in parallel. The application of a discrete Fourier transform in the final state of the quantum system yields the period of the function.

2. Database Search

Another problem that can be solved by quantum algorithms faster than conventional ones is the search of a database. If someone wants to find a particular item searching a random list of N items has to examine at least N/2 of them in order to ensure a 50% success probability.[8] In 1996 Lov Grover showed[18] that a quantum computer could perform this task in $\sqrt{N}$ steps. This is an increase of speed by a factor of $\sqrt{N}$.

3. Simulations of Quantum Systems

Quantum systems cannot be simulated with classical computers because Hilbert space grows exponentially with the number of particles included in the system. Feynman was the first to understand that fact and to propose in 1982 the construction of quantum computers for the simulation of quantum systems.[1,2] Several researchers have since showed that quantum systems can be simulated by quantum computers.

B. PROPOSED REALIZATIONS

Since 1982 when the field of quantum computation emerged most of the research was theoretical and there were no experimental breakthroughs. However, in the last few years this trend has changed. Experimental and theoretical developments have helped researchers to find and propose some possible realizations for quantum computers. A brief overview of two of these schemes is presented below.

1. Ion Trap Quantum Computer

One of the first promising prototypes for quantum computers is the ion trap proposed by Ignacio Cirac and Peter Zoller of the University of Innsbruck.[19] The basis for this scheme is a string of ions stored in a linear ion trap. A simplified schematic representation is depicted in Figure 3.1.

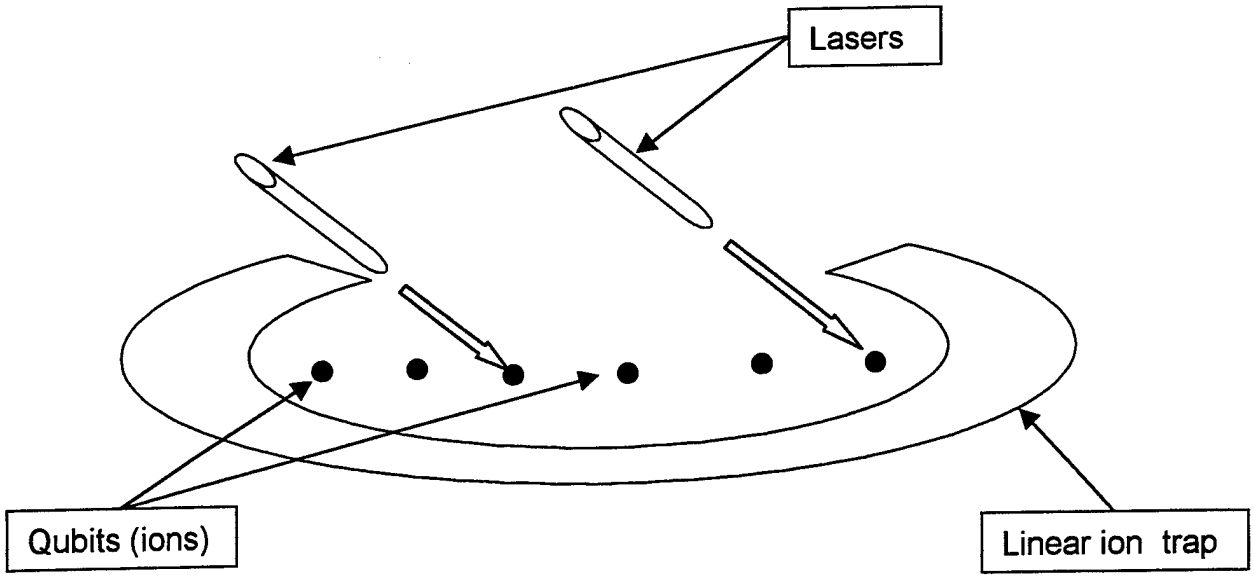

Figure 3.1 Ion-trap QC

In this proposal the internal states of trapped ions represent the qubits. The electrostatic repulsive interaction between ions provides the means of communication between qubits. Due to Coulomb interaction the linear chain of trapped ions has vibrational modes.[8] The number of normal modes is equal to the number of ions. The internal state of each ion can be altered by appropriate laser beams, which induce vibrations. These vibrations change the normal modes of the system. Thus, we have the transfer of information from one specific ion (qubit) to the normal mode of the system. An elaborate treatment of the ion trap proposal can be found in the references.

We will note that there are currently a lot of groups experimenting with this realization.[8] The results from the first experiments are promising.[20] The technology involved is feasible and already being used for other scientific purposes.[8] Finally the most promising aspect of ion traps is that they provide a

reliable measurement for the output states utilizing the quantum jump technique. This technique can detect the state of an ion with absolute accuracy and almost absolute efficiency.

2. Nuclear Magnetic Resonance (NMR)

Nuclear magnetic resonance (NMR) is considered today one of the major tools in synthetic chemistry.[8] It is used to study the properties of all states of matter except plasma. The field has been developed since 1940's.

The physical system used for NMR quantum computation[8] is a single molecule with two magnetically distinct nuclei. The qubits are represented by nuclear spins, while gate operations are performed by manipulations of the spins. The most important method for spin manipulations is the application of radio-frequency (RF) pulses. These pulses must have the appropriate power, duration and phase.

The above brief description consists the ideal NMR quantum computer. The signal produced from a single nucleus is very small and currently there are no available methods to detect it. In order to have a signal strong enough to be detected large number of molecules are needed. It is noted that current technology cannot detect signals generated by a small number of molecules, which is what we need for quantum computing.

For many years there were two basic problems that made NMR computation impossible, the preparation of the initial state and the measurement of the output. The preparation problem has to do with the fact that an ensemble

of 2-spin molecules in thermal equilibrium contains equally populated spin-up and spin-down states. This initial state is totally random and of course is not acceptable for a computation where a definite input state must be prepared (even as a superposition of other states). The measurement problem arises from the fact that for an NMR computer a large number of molecules is used and the only output you can measure is the ensemble average magnetization. You can't measure the output of a single qubit (molecule).

In 1997 research groups found solutions for both of these problems and since then there is a growing number of groups that search for possible implementations.[8]

It should be noted that NMR computation has a great advantage due to the long coherence times of the spin superposition states. This has as a result a reduction in decoherence problems and makes NMR an attractive candidate if the other problems will be resolved.

3. Cavity Quantum Electrodynamics (QED)

Finally, we note that a very promising approach to develop a universal quantum gate exploits the phenomena of cavity QED. In the next section we discuss the theoretical background necessary to understand cavity QED. As we have noted the operation of a quantum gate is controlled by the Hamiltonian of the system. In what follows, therefore, we will concentrate on deriving the Hamiltonian for a cavity QED system.

IV. CAVITY QUANTUM ELECTRODYNAMICS

A. GENERAL

One of the most accurate theories developed in this century is the theory of Quantum Electrodynamics (QED), which provides us with the appropriate tools to describe and predict the coupling between charged particles and electromagnetic fields. The concepts for the interaction of light and matter can describe all the physical phenomena except gravity and radioactivity, according to Feynman.

In this chapter we will provide the theoretical background of the interaction of atoms with a single mode field. This is necessary for the derivation of the Hamiltonian for the system that can be used to implement a 2-bit quantum gate.

B. DERIVATION OF HAMILTONIAN

1. Quantization of the Electromagnetic Field

The most elementary approach for the quantization of the electromagnetic field is by the means of harmonic oscillator. A field mode is equivalent to a harmonic oscillator. This treatment can be found in most quantum optics books but we followed the texts by Milonni[21] and Loudon.[22]

First we begin with a brief review for the harmonic oscillator in quantum mechanics.[23] The Hamiltonian for a harmonic oscillator is given by:

$$H = \frac{p^2}{2m} + \frac{1}{2} m\omega^2 q^2 \qquad (1)$$

where p and q are operators in a Hilbert space.

The Heisenberg equations of motion are of the same form as the classical Hamilton equations:

$$\dot{q} = (i\hbar)^{-1}[q, H] = \frac{p}{m} \qquad (2)$$

$$\dot{p} = (i\hbar)^{-1}[p, H] = -m\omega^2 q \qquad (3)$$

Now if we define the non-Hermitian operators α and α^+

$$\alpha = \frac{1}{\sqrt{2m\hbar\omega}}(p - im\omega q) \qquad (4)$$

$$\alpha^+ = \frac{1}{\sqrt{2m\hbar\omega}}(p + im\omega q) \qquad (5)$$

then q and p can be written as:

$$q = i\sqrt{\frac{\hbar}{2m\omega}}(\alpha - \alpha^+), \qquad (6)$$

$$p = \sqrt{\frac{m\hbar\omega}{2}}(\alpha + \alpha^+) \qquad (7)$$

and we can write the Hamiltonian as:

$$H = \frac{1}{2}\hbar\omega(\alpha\alpha^+ + \alpha^+\alpha) = (\frac{1}{2} + \alpha^+\alpha)\hbar\omega \qquad (8)$$

The eigenvalues of the operator $N = \alpha^+\alpha$ determine the energy levels of the harmonic oscillator, which are given by:

$$E_n = (n + \frac{1}{2})\hbar\omega \tag{9}$$

The second step is to show that a field mode is equivalent to the harmonic oscillator[21]. We assume that we work in vacuum where there are no sources and the Maxwell's equations are:

$$\nabla \cdot \mathbf{E} = 0 \tag{10}$$

$$\nabla \cdot \mathbf{B} = 0 \tag{11}$$

$$\nabla \times \mathbf{E} = -\frac{1}{c}\frac{\partial \mathbf{B}}{\partial t} \tag{12}$$

$$\nabla \times \mathbf{B} = \frac{1}{c}\frac{\partial \mathbf{E}}{\partial t} \tag{13}$$

We define the vector potential **A** such that $\mathbf{B} = \nabla \times \mathbf{A}$ and the scalar potential ϕ. Then we can see that equation (11) above is satisfied due to the fact that $\nabla \cdot (\nabla \times \mathbf{A}) = 0$. Also in order to satisfy equation (12) we must have that:

$$\mathbf{E} = -\frac{1}{c}\frac{\partial \mathbf{A}}{\partial t} - \nabla\varphi \tag{14}$$

and so we can write equation (13) as:

$$\nabla^2 \mathbf{A} - \frac{1}{c^2}\frac{\partial^2 \mathbf{A}}{\partial t^2} = 0 \tag{15}$$

We separate the variables by assuming that $\mathbf{A}(\mathbf{r},t) = \alpha(t)\mathbf{A}(\mathbf{r})$. Then defining the separation constant k and $\omega = ck$ and substituting in the above equation (15) we get:

$$\alpha(t)\nabla^2\mathbf{A}(\mathbf{r}) = \frac{1}{c^2}\ddot{\alpha}(t)\mathbf{A}(\mathbf{r}) \Rightarrow \frac{\nabla^2\mathbf{A}(\mathbf{r})}{\mathbf{A}(\mathbf{r})} = \frac{1}{c^2}\frac{\ddot{\alpha}(t)}{\alpha(t)} = -k^2 \Rightarrow$$

$$\Rightarrow \nabla^2\mathbf{A}(\mathbf{r}) + k^2\mathbf{A}(\mathbf{r}) = 0 \qquad (16)$$

$$\ddot{\alpha}(t) = -\omega^2\alpha(t)$$

The solutions to the equations (16) give us the following general solution:

$$\mathbf{A}(\mathbf{r},t) = \alpha(t)\mathbf{A}(\mathbf{r}) + \alpha^*(t)\mathbf{A}^*(\mathbf{r}) = \alpha(0)e^{-i\omega t}\mathbf{A}(\mathbf{r}) + \alpha^*(0)e^{i\omega t}\mathbf{A}^*(\mathbf{r}) \quad (17)$$

Then we can find expressions for the electric and magnetic field vectors in the case φ=0 (vacuum), using equation (14) and $\mathbf{B} = \nabla \times \mathbf{A}$, as:

$$\mathbf{E}(\mathbf{r},t) = -\frac{1}{c}\left[\dot{\alpha}(t)\mathbf{A}(\mathbf{r}) + \dot{\alpha}^*(t)\mathbf{A}^*(\mathbf{r})\right] \qquad (17)$$

$$\mathbf{B}(\mathbf{r},t) = \alpha(t)\nabla \times \mathbf{A}(\mathbf{r}) + \alpha^*(t)\nabla \times \mathbf{A}^*(\mathbf{r}) \qquad (18)$$

Then we can find the electromagnetic energy, by its definition, as follows:

$$U = \frac{1}{8\pi}\int d^3r(\mathbf{E}^2 + \mathbf{B}^2) = \frac{1}{8\pi}\{\frac{1}{c^2}\dot{\alpha}(t)^2\int d^3r\mathbf{A}(\mathbf{r})^2 + \frac{1}{c^2}\dot{\alpha}^*(t)^2\int d^3r\mathbf{A}^*(\mathbf{r})^2 + \frac{2}{c^2}|\dot{\alpha}(t)|^2\int d^3r|\mathbf{A}(\mathbf{r})|^2 +$$
$$+\alpha(t)^2\int d^3r[\nabla \times \mathbf{A}(\mathbf{r})]^2 + \alpha^*(t)^2\int d^3r[\nabla \times \mathbf{A}^*(\mathbf{r})]^2 + 2|\alpha(t)|^2\int d^3r|\nabla \times \mathbf{A}(\mathbf{r})|^2\}$$

Now we know that $\alpha(t) = \alpha(0)e^{-i\omega t}$, as it was defined above and so:

$$\dot{\alpha}(t) = -i\omega\alpha(t) \qquad \dot{\alpha}(t)^2 = -\omega^2\alpha(t)^2 \qquad \dot{\alpha}^*(t)^2 = -\omega^2\alpha^*(t)^2$$

Also in Appendix A we show that $\int d^3r[\nabla \times \mathbf{A}(\mathbf{r})]^2 = k^2\int d^3r\mathbf{A}(\mathbf{r})^2$

Finally we can assume that the function **A(r)** is normalized, so that $\int d^3r|\mathbf{A}(\mathbf{r})|^2 = 1$ and the equation for the electromagnetic energy becomes after these substitutions:

$$U = H_F = \frac{1}{8\pi}\int d^3r(\mathbf{E}^2 + \mathbf{B}^2) = \frac{k^2}{2\pi}|\alpha(t)|^2 \qquad (19)$$

This last equation is the Hamiltonian for the electromagnetic field.

Now if we define the quantities:

$$q(t) = \frac{i}{c\sqrt{4\pi}}\left[\alpha(t) - \alpha^*(t)\right] \qquad (20)$$

$$p(t) = \frac{k}{\sqrt{4\pi}}\left[\alpha(t) + \alpha^*(t)\right] \qquad (21)$$

the Hamiltonian becomes:

$$H_F = \frac{1}{2}\left(p^2 + \omega^2 q^2\right) \qquad (22)$$

Since we have define $\alpha(t) = \alpha(0)e^{-i\omega t}$ and $\alpha^*(t) = \alpha^*(0)e^{i\omega t}$ we have that:

$$\dot{\alpha}(t) = -i\omega\alpha(t), \qquad \dot{\alpha}^*(t) = i\omega\alpha^*(t)$$

From the equations (20) and (21) we can see that $\dot{q} = p$ and $\dot{p} = -\omega^2 q$. The same result is obtained if we apply the Hamilton equations of motion for the Hamiltonian obtained in equation (22):

$$\dot{q} = \frac{\partial H}{\partial p} = p \text{ and } \dot{p} = -\frac{\partial H}{\partial q} = -\omega^2 q$$

So the defined quantities q and p are canonically conjugate coordinate and momentum variables respectively. We can now see the direct mathematical equivalence between equation (22), which describes a field mode with frequency ω and the equation (1) for the harmonic oscillator of frequency ω and mass m. Equation (22) is just a harmonic oscillator with unit mass.

Now in order to transform the above classical Hamiltonian for the field mode to a quantum mechanical one we just follow what we did for the harmonic oscillator. Thus we define the lowering and raising operators α and α^+ similar to the ones defined in equations (4) and (5), but with unity mass. Then by direct comparison with equations (20) and (21) we can find that we have to replace the classical variables $\alpha(t)$ and $\alpha^*(t)$ with respective quantum mechanical operators:

$$\frac{i\alpha(t)}{c\sqrt{4\pi}} = i\alpha(t)\sqrt{\frac{\hbar}{2\omega}} \Rightarrow \alpha(t) = \alpha(t)\sqrt{\frac{2\pi\hbar c^2}{\omega}} \qquad (23)$$

$$\frac{i\alpha^*(t)}{c\sqrt{4\pi}} = i\alpha^+(t)\sqrt{\frac{\hbar}{2\omega}} \Rightarrow \alpha(t) = \alpha^+(t)\sqrt{\frac{2\pi\hbar c^2}{\omega}} \qquad (24)$$

So we can find that the Hamiltonian for the quantized field mode is:

$$H = \frac{1}{2}\hbar\omega(\alpha\alpha^+ + \alpha^+\alpha) = (\frac{1}{2} + \alpha^+\alpha)\hbar\omega \qquad (25)$$

It is noted that from now on α and α^+ are operators.

Also the classical vector potential as well the classical electric and magnetic fields are now given by new equations and they are now operators in the quantum picture:

$$\mathbf{A}(\mathbf{r},t)=\left(\sqrt{\frac{2\pi\hbar c^2}{\omega}}\right)\left[\alpha(t)\mathbf{A}(\mathbf{r})+\alpha^{+}(t)\mathbf{A}^{*}(\mathbf{r})\right] \qquad (26)$$

$$\mathbf{E}(\mathbf{r},t)=i\left(\sqrt{2\pi\hbar\omega}\right)\left[\alpha(t)\mathbf{A}(\mathbf{r})-\alpha^{+}(t)\mathbf{A}^{*}(\mathbf{r})\right] \qquad (27)$$

$$\mathbf{B}(\mathbf{r},t)=\left(\sqrt{\frac{2\pi\hbar c^2}{\omega}}\right)\left[\alpha(t)\nabla\times\mathbf{A}(\mathbf{r})+a^{+}(t)\nabla\times\mathbf{A}^{*}(\mathbf{r})\right] \qquad (28)$$

We can also see that the energy eigenvalues are given again by:

$$E_n=(n+\frac{1}{2})\hbar\omega \qquad \text{n=0,1,2,...} \qquad (29)$$

We see from this last equation that even for n=0 (no photons) the vacuum has energy $\frac{1}{2}\hbar\omega$. This is one of the most interesting predictions of QED, the existence of zero point electromagnetic field.

Also we note that in all stationary states the vacuum expectation values for **E** and **B** fields are zero:

$$\langle\mathbf{E}(\mathbf{r},t)\rangle=\langle\mathbf{B}(\mathbf{r},t)\rangle=0 \qquad (30)$$

Up to this point we have talked about a single field mode only. We can make the transition now for a multimode field. Even though it is not necessary for what we describe later we show here that the proof above can be generalized.

The conditions we have set so far for the field in free space are that the field intensity is independent of position, the spatial part of vector potential **A(r)** satisfies the Helmholtz equation $\nabla^2\mathbf{A}(\mathbf{r})+k^2\mathbf{A}(\mathbf{r})=\mathbf{0}$ and the Coulomb gauge $\nabla\cdot\mathbf{A}(\mathbf{r},t)=0$.

A function that satisfies the above relations is given by:

$$\mathbf{A}(\mathbf{r}) = e^{i\mathbf{k}\mathbf{r}}\hat{\mathbf{e}}_{\mathbf{k}} \tag{31}$$

with $\hat{\mathbf{e}}_{\mathbf{k}}$ a unit vector and $\hat{\mathbf{e}}_{\mathbf{k}} \cdot \mathbf{k} = 0$

If we divide the space into cubes of volume L^3 and use the boundary condition for the vector potential:

$$\mathbf{A}(x+L, y+L, z+L, t) = \mathbf{A}(x, y, z, t) \tag{32}$$

we have that :

$$k_x = \frac{2\pi n_x}{L}, \quad k_y = \frac{2\pi n_y}{L}, \quad k_z = \frac{2\pi n_z}{L}, \; n_x, n_y, n_z \text{ integers} \tag{33}$$

In order to satisfy the normalization condition $\int d^3r |\mathbf{A}(\mathbf{r})|^2 = 1$ the vector potential **A(r)** must have the form:

$$\mathbf{A}_{\mathbf{k}}(\mathbf{r}) = \frac{\mathbf{1}}{\sqrt{V}} e^{i\mathbf{k}\mathbf{r}}\hat{\mathbf{e}}_{\mathbf{k}} \tag{34}$$

The unit vector $\hat{\mathbf{e}}_{\mathbf{k}}$ specifies also the polarization of the field. From the fact that $\hat{\mathbf{e}}_{\mathbf{k}} \cdot \mathbf{k} = 0$ we can see that $\hat{\mathbf{e}}_{\mathbf{k}}$ can take two values (with opposite directions) $\hat{\mathbf{e}}_{\mathbf{k}1}, \hat{\mathbf{e}}_{\mathbf{k}2}$ with:

$$\hat{\mathbf{e}}_{\mathbf{k}1} \cdot \hat{\mathbf{e}}_{\mathbf{k}2} = 0, \qquad \hat{\mathbf{e}}_{\mathbf{k}1}^2 = \hat{\mathbf{e}}_{\mathbf{k}2}^2 = 1$$

Each of these values represent the polarizations of the field. So now we can write the functions for the mode from equation (34) as:

$$\mathbf{A}_{\mathbf{k}\lambda}(\mathbf{r}) = \frac{\mathbf{1}}{\sqrt{V}} e^{i\mathbf{k}\mathbf{r}}\hat{\mathbf{e}}_{\mathbf{k}\lambda}, \text{ (where } \lambda=1,2) \tag{35}$$

The equation (26) above for vector potential can now be rewritten as:

$$\mathbf{A}_{\mathbf{k}\lambda}(\mathbf{r},t)=\left(\sqrt{\frac{2\pi\hbar c^2}{\omega_k V}}\right)\left[\alpha_{\mathbf{k}\lambda}(t)e^{i\mathbf{k}\mathbf{r}}+\alpha^{+}_{\mathbf{k}\lambda}(t)e^{-i\mathbf{k}\mathbf{r}}\right]\hat{\mathbf{e}}_{\mathbf{k}\lambda}\Rightarrow$$

$$\Rightarrow \mathbf{A}_{\mathbf{k}\lambda}(\mathbf{r},t)=\left(\sqrt{\frac{2\pi\hbar c^2}{\omega_k V}}\right)\left[\alpha_{\mathbf{k}\lambda}(0)e^{i(\mathbf{k}\mathbf{r}-\omega t)}+\alpha^{+}_{\mathbf{k}\lambda}(0)e^{-i(\mathbf{k}\mathbf{r}-\omega t)}\right]\hat{\mathbf{e}}_{\mathbf{k}\lambda} \quad (36)$$

In the above equation $\omega_k = kc$ (as defined before) and $a_{\mathbf{k}\lambda}, a^{+}_{\mathbf{k}\lambda}$ are the photon annihilation and creation operators.

The artificial boundary condition we applied for the field suggests that we have an infinite number of modes. Equation (36) describes one mode only (for a specific k). So the total potential would be the sum over all possible modes $\mathbf{k}_\lambda$, due to the linearity of Maxwell's equations:

$$\mathbf{A}_{\mathbf{k}\lambda}(\mathbf{r},t)=\sum_{\mathbf{k}\lambda}\left(\sqrt{\frac{2\pi\hbar c^2}{\omega_k V}}\right)\left[\alpha_{\mathbf{k}\lambda}(0)e^{i(\mathbf{k}\mathbf{r}-\omega t)}+\alpha^{+}_{\mathbf{k}\lambda}(0)e^{-i(\mathbf{k}\mathbf{r}-\omega t)}\right]\hat{\mathbf{e}}_{\mathbf{k}\lambda} \quad (37)$$

Finally we can write the Hamiltonian as the sum over all possible modes and it will have the form of the Hamiltonian for one mode:

$$H_F=\sum_{\mathbf{k}\lambda}\left(\frac{\mathbf{1}}{\mathbf{2}}+\alpha^{+}_{\mathbf{k}\lambda}\alpha_{\mathbf{k}\lambda}\right)\hbar\omega_k \quad (38)$$

From our assumptions for the normalization of the modes and the definitions for the operators $a_{\mathbf{k}\lambda}, a^{+}_{\mathbf{k}\lambda}$ we can write the following important relations:

$$\int_V d^3r\,\mathbf{A}_{\mathbf{k}\lambda}\cdot\mathbf{A}^{*}_{\mathbf{k}\lambda}=\delta^3_{\mathbf{k},\mathbf{k}'}\delta_{\lambda,\lambda'} \quad (39)$$

$$\left[\alpha_{\mathbf{k}\lambda}(t), \alpha^{+}_{\mathbf{k}'\lambda'}(t)\right] = \delta^{3}_{\mathbf{k},\mathbf{k}'}\delta_{\lambda,\lambda'} \tag{40}$$

In our approach $\mathbf{A}_{\mathbf{k}\lambda}$ represent an infinite number of discrete mode functions that satisfy the artificial imposed boundary conditions. It would be nice to have continuous mode functions, but we must point out that this does not add anything in the physical meaning. The quantization of the field can be done by a different approach with quantum field theory, which is a more elaborated treatment and also gives the continuous mode functions. In any case we will not need later the quantized field for infinite number of modes but for a single mode only.

2. Interaction of Atoms with Single Mode Field

Now that we have derived the quantization of the electromagnetic field in vacuum we can take the next step which has to do with the derivation of a theory that can describe the interactions between atoms and the field. This is the non-relativistic QED theory.[21,22] We are still assuming that we work in the Coulomb gauge, while we will make some further assumptions in order to reduce the terms that will appear in the equations.

In our derivation we will use again the Hamiltonian and the Hamilton equations of motion. It is known that for a charged particle in a field the Hamiltonian is:

$$H = \mathbf{p}\cdot\mathbf{v} - \frac{1}{2}m\mathbf{v}^{2} + e\phi - \frac{e}{c}\mathbf{A}\cdot\mathbf{v} \tag{41}$$

where **p** we must remember is the canonical momentum described by:

$$\mathbf{p} = m\mathbf{v} + \frac{e}{c}\mathbf{A} \tag{42}$$

so that the Hamiltonian can take the form:

$$H = \frac{1}{2m}\left(\mathbf{p} - \frac{e}{c}\mathbf{A}\right)^2 + e\phi \tag{43}$$

Now this last equation determines the time evolution of the particle's motion. Our goal is to find a Hamiltonian that will determine also the evolution of the electromagnetic field. To do that we assume that the combined Hamiltonian should have two terms, one obtained from the electromagnetic energy of the field and the other obtained from the kinetic energy of the particle.

We can see that the kinetic energy of the particle can be written by the equation (42) above as:

$$\frac{1}{2}m\mathbf{v}^2 = \frac{1}{2m}\left(\mathbf{p} - \frac{e}{c}\mathbf{A}\right)^2 \tag{44}$$

We also recall the Hamiltonian found for the field, so we can add these terms to express the total Hamiltonian as:

$$H = \frac{1}{2m}\left(\mathbf{p} - \frac{e}{c}\mathbf{A}\right)^2 + \frac{1}{8\pi}\int d^3r(\mathbf{E}^2 + \mathbf{B}^2) \tag{45}$$

Comparing equations (43) and (45) above we can see that there is a term missing, specifically the term eφ. In Appendix B we present a treatment, which proves that this term is included implicitly in equation (45) and that if we want it to appear explicitly in the Hamiltonian we have to express differently the form of the electromagnetic energy of the field.

As shown in Appendix B the Hamiltonian for the system of particle and the field can be expressed as:

$$H = \frac{1}{2m}\left(\mathbf{p} - \frac{e}{c}\mathbf{A}\right)^2 + e\phi + \frac{1}{8\pi}\int d^3r\left(\mathbf{E}^{\perp 2} + \mathbf{B}^2\right) \qquad (46)$$

where $\mathbf{E}^{\perp}$ is the transverse part of the electric field vector.

We wish now to simplify further the above Hamiltonian using the electric dipole approximation.[21,22] In this approximation we can assume that the vector potential **A** is independent of position and so we can ignore the spatial variations of vector potential when we expand the square bracket in equation (46). So we can write the Hamiltonian as:

$$H = \frac{\mathbf{p}^2}{2m} - \frac{e}{mc}\mathbf{A}\cdot\mathbf{p} + \frac{e^2}{2mc^2}\mathbf{A}^2 + V(\mathbf{x}) + \frac{1}{8\pi}\int d^3r\left(\mathbf{E}^{\perp 2} + \mathbf{B}^2\right) \qquad (47)$$

where we have introduced $V = e\phi$.

Equation (47) is known as the minimal-coupling Hamiltonian. The interaction between the atom and the field is contained in the terms:

$$\frac{e}{mc}\mathbf{A}\cdot\mathbf{p} + \frac{e^2}{2mc^2}\mathbf{A}^2$$

We also note that there are higher order interactions (quadropolar,etc.) but their contribution is very small and can be neglected. This is the reason we used the dipole approximation for the derivation of equation (47).

After all these steps we can now proceed with the quantization of the derived classical Hamiltonian. We define the following Hamiltonians for the particle and the field respectively:

$$H_a = \frac{\mathbf{p}^2}{2m} + V(\mathbf{x}) \tag{48}$$

$$H_F = \sum_{\mathbf{k}\lambda} \left(\alpha^+_{\mathbf{k}\lambda} \alpha_{\mathbf{k}\lambda} + \frac{1}{2} \right) \hbar\omega_k \tag{49}$$

Then we replace the classical variables **E**, **B**, **p** and **x** by quantum mechanical operators. So the total Hamiltonian of equation (47) can now be written using equations (26),(48),(49) as:

$$H = H_a + H_F - \frac{e}{mc} \sum_{\mathbf{k}\lambda} \sqrt{\left(\frac{2\pi\hbar c^2}{\omega_k V} \right)} \left(\alpha_{\mathbf{k}\lambda} + \alpha^+_{\mathbf{k}\lambda} \right) \mathbf{p} \cdot \hat{\mathbf{e}}_{\mathbf{k}\lambda} +$$

$$+ \frac{e^2}{2mc^2} \sum_{\mathbf{k}\lambda} \sum_{\mathbf{k}'\lambda'} \frac{2\pi\hbar c^2}{V} \sqrt{\left(\frac{1}{\omega_k \omega_{k'}} \right)} \left(\alpha_{\mathbf{k}\lambda} + \alpha^+_{\mathbf{k}\lambda} \right) \hat{\mathbf{e}}_{\mathbf{k}\lambda} \cdot \left(\alpha_{\mathbf{k}'\lambda'} + \alpha^+_{\mathbf{k}'\lambda'} \right) \hat{\mathbf{e}}_{\mathbf{k}'\lambda'} \tag{50}$$

It should be noted that since we have assumed the condition of the Coulomb gauge we only quantize the transverse electromagnetic field in equation (50). The energy of the longitudinal field has been replaced by the instantaneous Coulomb interactions among the particles (please see also Appendix B).

In the Hamiltonian of equation (50) we notice that the radiative part is quantized and expressed in terms of photon creation and annihilation operators. It would be useful to do the same with the terms of Hamiltonian that involve the

particle and their interaction with the field. Then we would have the entire Hamiltonian in terms of destruction and creation operators for both particle and field states. Before we proceed with the quantization we notice that the last term $\frac{e^2}{2mc^2}\mathbf{A}^2$ in equation (50) can be neglected. This term is already quantized and it will not be affected by our second quantization, since it does not explicitly involve any atomic operators. Thus, its contribution to the coupling between the atom and the field is very small.[22]

We can now recall that the completeness theorem[6] for the basis vectors $|n\rangle$ requires that $\sum_n |n\rangle\langle n| = 1 = \sum_n \sigma_{nn}$ and that $H|n\rangle = E_n|n\rangle$, $\langle n|F|m\rangle = F_{n,m}$, where $|n\rangle$ are the energy eigenstates, F is an operator and σ is the density operator for particle states.

Then we can express the Hamiltonian for the particle, applying the completeness theorem twice, as:

$$H_a = \left[\sum_n |n\rangle\langle n|\right] H_a \left[\sum_m |m\rangle\langle m|\right] = \sum_{n.m} |n\rangle\langle m|\langle n|H_a|m\rangle = \sum_{n,m} |n\rangle\langle m|E_m\langle n|m\rangle = \sum_n |n\rangle\langle n|E_n = \sum_n \sigma_{nn}E_n$$

We can develop a similar expression for the momentum operator **p**:

$$\mathbf{p} = \left[\sum_n |n\rangle\langle n|\right]\mathbf{p}\left[\sum_m |m\rangle\langle m|\right] = \sum_{n.m} |n\rangle\langle n|\mathbf{p}|m\rangle\langle m| = \sum_{n,m} |n\rangle\mathbf{p}_{n,m}\langle m| = \sum_{n,m} \mathbf{p}_{n,m}|n\rangle\langle m| = \sum_{n,m} \mathbf{p}_{n,m}\sigma_{n,m}$$

Thus, we can write the total Hamiltonian as:

$$H = \sum_n \sigma_{nn}E_n + \sum_{\mathbf{k}\lambda}\left(\alpha^+_{\mathbf{k}\lambda}\alpha_{\mathbf{k}\lambda} + \frac{1}{2}\right)\hbar\omega_k - \frac{e}{mc}\sum_{\mathbf{k}\lambda}\sum_{n,m}\sqrt{\left(\frac{2\pi\hbar c^2}{\omega_k V}\right)}\left(\alpha_{\mathbf{k}\lambda} + \alpha^+_{\mathbf{k}\lambda}\right)\mathbf{p}_{n,m}\sigma_{n,m} \quad (51)$$

Now we define the coupling constant for the interaction called g as:

$$g_{\mathbf{k}\lambda nm} = \frac{e}{m}\sqrt{\frac{2\pi}{\hbar\omega_k V}}\mathbf{p}_{n,m}\cdot\hat{\mathbf{e}}_{\mathbf{k}\lambda} \qquad (52)$$

It is noted that in equation (52) there are no diagonal terms, since they vanish due to the fact that the operator p_{nm} has odd parity.[22] This fact will be used below when we will express this Hamiltonian for the two-state atom.

Then we can rewrite equation (51) as:

$$H = \sum_n \sigma_{nn}E_n + \sum_{\mathbf{k}\lambda}\left(\alpha^+_{\mathbf{k}\lambda}\alpha_{\mathbf{k}\lambda} + \frac{1}{2}\right)\hbar\omega_k - \hbar\sum_{\mathbf{k}\lambda}\sum_{n,m} g_{\mathbf{k}\lambda nm}\left(\alpha_{\mathbf{k}\lambda} + \alpha^+_{\mathbf{k}\lambda}\right)\sigma_{n,m} \qquad (53)$$

This Hamiltonian is now quantized and expressed in terms of operators only. Now we can proceed and apply this for a two-state atom.

The atom has two accessible states $|0\rangle$ and $|1\rangle$. Then equation (53) can be simplified. The energy eigenvalues for each state are E_0 and E_1 and we have that $E_1 - E_0 = \hbar\omega_0$. We also know that $\sigma_{00} + \sigma_{11} = 1$, from the definition of σ_{nm} above. Then we have:

$$\sum_n E_n\sigma_{nn} = E_1\sigma_{11} + E_0\sigma_{00} = \frac{1}{2}E_1(\sigma_{11} + 1 - \sigma_{00}) + \frac{1}{2}E_0(\sigma_{00} + 1 - \sigma_{11}) =$$

$$= \frac{1}{2}(E_1 - E_0)(\sigma_{11} - \sigma_{00}) + \frac{1}{2}(E_1 + E_0) = \frac{1}{2}\hbar\omega_0\sigma_z + \frac{1}{2}(E_1 + E_0) \qquad (54)$$

In equation (54) we defined:

$$\sigma_z \equiv \sigma_{11} - \sigma_{00} \qquad (55)$$

Also we have that:

$$\sum_{n,m} g_{\mathbf{k}\lambda nm}\sigma_{nm} = g_{\mathbf{k}\lambda 01}\sigma_{01} + g_{\mathbf{k}\lambda 01}\sigma_{01} = -g_{\mathbf{k}\lambda 01}(\sigma_{01} - \sigma_{10}) \tag{56}$$

Now we define:

$$\sigma_y = i(\sigma_{01} - \sigma_{10}) \tag{57}$$

$$\sigma_x = \sigma_{01} + \sigma_{10} \tag{58}$$

$$g_{\mathbf{k}\lambda} = -ig_{\mathbf{k}\lambda 10} \tag{59}$$

Then using equations (57) and (59) equation (56) can be written as:

$$\sum_{n,m} g_{\mathbf{k}\lambda nm}\sigma_{nm} = -g_{\mathbf{k}\lambda}\sigma_y \tag{60}$$

It is shown in Appendix C that the two-state operators $\sigma_x, \sigma_y, \sigma_z$ satisfy the Pauli algebra for spin-1/2 particle:

$$[\sigma_x, \sigma_y] = 2i\sigma_z,\ [\sigma_y, \sigma_z] = 2i\sigma_x,\ [\sigma_z, \sigma_x] = 2i\sigma_y \tag{61}$$

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = 1 \tag{62}$$

We can also define the operators:

$$\sigma \equiv \sigma_{01}, \qquad \sigma^+ \equiv \sigma_{10} \tag{63}$$

Then we have the following properties for these operators:

$$\sigma|1\rangle = |0\rangle\langle 1|1\rangle = |0\rangle \qquad \sigma^+|0\rangle = |1\rangle\langle 0|0\rangle = |1\rangle \tag{64}$$

$$\sigma|0\rangle = |0\rangle\langle 1|0\rangle = 0 \qquad \sigma^+|1\rangle = |1\rangle\langle 0|1\rangle = 0 \tag{65}$$

$$[\sigma^+, \sigma] = \sigma_z \qquad [\sigma, \sigma_z] = 2\sigma \tag{66}$$

From the above properties, σ and σ^+ are called atomic lowering and raising operators respectively.

We are now ready to write the Hamiltonian of equation (53) in terms of these operators using equations (54), (56), (57), (60) and (63) as:

$$H = \frac{1}{2}\hbar\omega_0\sigma_z + \sum_{k\lambda}\hbar\omega_k\alpha_{k\lambda}^+\alpha_{k\lambda} + i\hbar\sum_{k\lambda}g_{k\lambda}(\alpha_{k\lambda} + \alpha_{k\lambda}^+)(\sigma - \sigma^+) \qquad (67)$$

In equation (67) we omitted the terms $\frac{1}{2}(E_1 + E_0)$ and $\sum_{k\lambda}\frac{1}{2}\hbar\omega_k$, since there are constants and do not affect the evolution of the system.

Finally, since we are interested in the interaction of atom with a single mode field we can further simplify equation (67) and write it as:

$$H = \frac{1}{2}\hbar\omega_0\sigma_z + \hbar\omega\alpha^+\alpha + i\hbar g(\alpha + \alpha^+)(\sigma - \sigma^+) \qquad (68)$$

This last equation is our final Hamiltonian that describes the interaction of the two-state atom with a single mode field. This is our starting point for describing the evolution of the proposed cavity QED quantum gate.

V. REALIZATION FOR 2-BIT UNIVERSAL GATE

In the previous Chapter we derived the Hamiltonian for the interaction between a two-state atom and a single mode field. In this Chapter we introduce some further approximations and we derive the Hamiltonian of the so called Jaynes-Cummings model.[21] Then we calculate the upper and lower state occupation probabilities for the two-state atom. Finally we describe a proposed scheme for a universal gate based on the above model.

A. CALCULATION OF STATE OCCUPATION PROBABILITIES

As a starting point we use the Hamiltonian of equation (68) of Chapter IV:

$$H = \frac{1}{2}\hbar\omega_0\sigma_z + \hbar\omega\alpha^+\alpha + i\hbar g(\alpha + \alpha^+)(\sigma - \sigma^+) \qquad (1)$$

One of the most useful approximations in the theory of two-state atoms is the rotating wave approximation (RWA).[24] This approximation is used here to reduce the Hamiltonian of equation (1). The RWA applies to the third term of above equation, which is the interaction term between atom and the field. We expand this term and find:

$$(\alpha + \alpha^+)(\sigma - \sigma^+) = \alpha\sigma - \alpha\sigma^+ + \alpha^+\sigma - \alpha^+\sigma^+ \qquad (2)$$

Now we consider the evolution of these operators using the Heisenberg picture without the coupling constant g (g=0).

The time dependence for the photon annihilation and creation operators has already been introduced in Chapter IV as:

$$\alpha(t) = \alpha(0)e^{-i\omega t} \qquad \alpha^+(t) = \alpha^+(0)e^{i\omega t} \tag{3}$$

The atomic lowering and raising operators have a similar time dependence:

$$\sigma(t) = \sigma(0)e^{-i\omega_0 t} \qquad \sigma^+(t) = \sigma^+(0)e^{i\omega_0 t} \tag{4}$$

Then, in the absence of coupling each term of equation (2) above becomes, using equations (3) and (4):

$$\alpha\sigma^+ = \alpha(0)\sigma^+(0)e^{-i(\omega-\omega_0)t} \tag{5}$$

$$\alpha^+\sigma = \alpha^+(0)\sigma(0)e^{i(\omega-\omega_0)t} \tag{6}$$

$$\alpha^+\sigma^+ = \alpha^+(0)\sigma^+(0)e^{i(\omega+\omega_0)t} \tag{7}$$

$$\alpha\sigma = \alpha(0)\sigma(0)e^{-i(\omega+\omega_0)t} \tag{8}$$

We can see that when we are interested for the case when $\omega = \omega_0$ (resonant and near resonant frequencies), the terms $\alpha^+\sigma^+$ and $\alpha\sigma$ in equations (7) and (8) are rapidly varying and their average tends to zero. These terms can be neglected. In contrast we see that the rest two terms $\alpha\sigma^+$ and $\alpha^+\sigma$ in equations (5) and (6) have a different time dependence and their average value near resonance is not zero. Thus we keep these two terms in the Hamiltonian. It is also noted that we have assumed the coupling between atom and field is very weak (g is very small number) otherwise the time dependence of the operators would be different and the RWA could not be applied.

We can also note the physical meaning[21,24] of the RWA. The term $\alpha\sigma^+$ represents the absorption of a photon and the excitation of the atom from lower to upper state. The term $\alpha^+\sigma$ represents the transition of the atom from upper to lower state and the emission of a photon. The term $\alpha\sigma$ represents the absorption of a photon and the transition from upper to lower state, while the term $\alpha^+\sigma^+$ describes the emission of a photon and the excitation of the atom. There are cases where the RWA can not be applied[21] but for our purposes is suitable. So we can now write the Hamiltonian of equation (1) as follows:

$$H = \frac{1}{2}\hbar\omega_0\sigma_z + \hbar\omega\alpha^+\alpha - i\hbar g(\sigma^+\alpha - \alpha^+\sigma) \qquad (9)$$

This last equation is the Jaynes-Cummings model (first presented by Jaynes and Cummings in 1963). Jaynes and Cummings used the dressed-state formalism to calculate the occupation probabilities for the atom.[21] We know that a given problem in quantum mechanics can be treated in different representation forms.[6,23] In the Schrödinger picture the time dependence is carried by the wave function, while in Heisenberg picture the time dependence is carried by the operators. The form of the Hamiltonian is the same as equation (9) for both pictures, as it is showed in textbooks[22], except the fact that the operators would be time dependent (for Heisenberg). Finally we note that another picture is the interaction representation[22], where both operators and wave function are time dependent.

We will work in the Schrödinger picture to calculate the occupation probabilities.

Since we are interested for the interaction of an excited atom with the single mode field, we assume that at time t=0 the atom is in the excited state $|1\rangle$ and the field has n photons present so it is in the state $|n\rangle$. The form of the wave function used is:

$$|\psi(t)\rangle = (A_{1n}(t)|1\rangle|n\rangle + B_{0n+1}(t)|0|n+1\rangle\rangle)e^{-i(n+\frac{1}{2})\omega t} \qquad (10)$$

We use the Schrödinger equation:

$$i\hbar\frac{\partial|\psi(t)\rangle}{\partial t} = H|\psi(t)\rangle \qquad (11)$$

We will substitute equation (10) into (11) and then we will project on the states $|1\rangle|n\rangle$ and $|0\rangle|n+1\rangle$ to get the equations for A_{1n} and B_{0n+1}. We know that the $|A_{1n}|^2$ and $|B_{0n+1}|^2$ will give us the occupation probabilities for the two states.

So first we calculate the left hand of equation (11):

$$i\hbar\frac{\partial|\psi(t)\rangle}{\partial t} = i\hbar\left(\dot{A}_{1n}(t)|1\rangle|n\rangle + \dot{B}_{0n+1}(t)|0\rangle|n+1\rangle\right)e^{-i(n+\frac{1}{2})\omega t} -$$

$$-i\hbar i\left(n+\frac{1}{2}\right)\omega(A_{1n}(t)|1\rangle|n\rangle + B_{0n+1}(t)|0|n+1\rangle\rangle)e^{-i(n+\frac{1}{2})\omega t} \qquad (12)$$

Then we have to calculate the right hand of equation (11). To do that we will use the following relations for the atomic operators who are proved in Chapter IV and Appendix C:

$$\sigma|1\rangle = |0\rangle \qquad \sigma|0\rangle = 0 \qquad \sigma^+|0\rangle = |1\rangle \qquad \sigma^+|1\rangle = 0 \tag{13}$$

$$\sigma_z|0\rangle = -|0\rangle \qquad \sigma_z|1\rangle = |1\rangle \tag{14}$$

Also we know the equations for the field operators:

$$\alpha|n+1\rangle = \sqrt{n+1}|n\rangle \qquad \alpha^+|n\rangle = \sqrt{n+1}|n+1\rangle \tag{15}$$

Then we can write for the right hand side of equation (11) using (13)-(15):

$$H|\psi(t)\rangle = \left(\frac{1}{2}\hbar\omega_0 + n\hbar\omega\right)\left(A_{1n}(t)|1\rangle|n\rangle\right)e^{-i(n+\frac{1}{2})\omega t} +$$

$$+\left[-\frac{1}{2}\hbar\omega_0 + (n+1)\hbar\omega\right]\left(B_{0n+1}(t)|0\rangle|n+1\rangle\right)e^{-i(n+\frac{1}{2})\omega t} +$$

$$+\left(-i\hbar g A_{1n}(t)\sigma^+\alpha|1\rangle|n\rangle - i\hbar g B_{0n+1}(t)\sigma^+\alpha|0\rangle|n+1\rangle\right)e^{-i(n+\frac{1}{2})\omega t} +$$

$$+\left(i\hbar g A_{1n}(t)\alpha^+\sigma|1\rangle|n\rangle + i\hbar g B_{0n+1}(t)\alpha^+\sigma|0\rangle|n+1\rangle\right)e^{-i(n+\frac{1}{2})\omega t} \Rightarrow$$

$$\Rightarrow H|\psi(t)\rangle = \left(\frac{1}{2}\hbar\omega_0 + n\hbar\omega\right)\left(A_{1n}(t)|1\rangle|n\rangle\right)e^{-i(n+\frac{1}{2})\omega t} +$$

$$+\left[-\frac{1}{2}\hbar\omega_0 + (n+1)\hbar\omega\right]\left(B_{0n+1}(t)|0\rangle|n+1\rangle\right)e^{-i(n+\frac{1}{2})\omega t} +$$

$$+\left(-i\hbar g B_{0n+1}(t)\sqrt{n+1}|1\rangle|n\rangle + i\hbar g A_{1n}(t)\sqrt{n+1}|0\rangle|n+1\rangle\right)e^{-i(n+\frac{1}{2})\omega t} \tag{16}$$

Now we substitute equations (12) and (16) in (11) and project onto the states $|1\rangle|n\rangle$ and $|0\rangle|n+1\rangle$. Then due to the orthogonality relations we have the following equations:

$$i\hbar\langle n|\langle 1|\Big[(\dot{A}_{1n}(t)|1\rangle|n\rangle+\dot{B}_{0n+1}(t)|0\rangle|n+1\rangle)-i\hbar(n+\frac{1}{2})\omega(A_{1n}(t)|1\rangle|n\rangle+B_{0n+1}(t)|0\rangle|n+1\rangle\Big]e^{-i(n+\frac{1}{2})\omega t}=$$

$$=\langle n|\langle 1|\Big[\Big(\frac{1}{2}\hbar\omega_0+n\hbar\omega\Big)A_{1n}(t)|1\rangle|n\rangle+\Big(-\frac{1}{2}\hbar\omega_0+(n+1)\hbar\omega\Big)B_{0n+1}(t)|0\rangle|n+1\rangle\Big]e^{-i(n+\frac{1}{2})\omega t}-$$

$$-i\hbar g\langle n|\langle 1|\Big[\Big(\sqrt{n+1}B_{0n+1}(t)|1\rangle|n\rangle\Big)-\Big(\sqrt{n+1}A_{1n}(t)|0\rangle|n+1\rangle\Big)\Big]e^{-i(n+\frac{1}{2})\omega t}\Rightarrow$$

$$\Rightarrow i\hbar\dot{A}_{1n}(t)+\Big(n+\frac{1}{2}\Big)\hbar\omega A_{1n}=\Big(\frac{1}{2}\omega_0+n\omega\Big)\hbar A_{1n}(t)-i\hbar g\sqrt{n+1}B_{0n+1}(t)\Rightarrow$$

$$\Rightarrow\dot{A}_{1n}(t)=\frac{i}{2}(\omega-\omega_0)-g\sqrt{n+1}B_{0n+1}(t)\qquad(17)$$

$$i\hbar\langle n+1|\langle 0|\Big[(\dot{A}_{1n}(t)|1\rangle|n\rangle+\dot{B}_{0n+1}(t)|0\rangle|n+1\rangle)-i\hbar(n+\frac{1}{2})\omega(A_{1n}(t)|1\rangle|n\rangle+B_{0n+1}(t)|0\rangle|n+1\rangle\Big]e^{-i(n+\frac{1}{2})\omega t}=$$

$$=\langle n+1|\langle 0|\Big[\Big(\frac{1}{2}\hbar\omega_0+n\hbar\omega\Big)A_{1n}(t)|1\rangle|n\rangle+\Big(-\frac{1}{2}\hbar\omega_0+(n+1)\hbar\omega\Big)B_{0n+1}(t)|0\rangle|n+1\rangle\Big]e^{-i(n+\frac{1}{2})\omega t}-$$

$$-i\hbar g\langle n+1|\langle 0|\Big[\Big(\sqrt{n+1}B_{0n+1}(t)|1\rangle|n\rangle\Big)-\Big(\sqrt{n+1}A_{1n}(t)|0\rangle|n+1\rangle\Big)\Big]e^{-i(n+\frac{1}{2})\omega t}\Rightarrow$$

$$\Rightarrow i\hbar\dot{B}_{0n+1}(t)+\Big(n+\frac{1}{2}\Big)\hbar\omega B_{0n+1}(t)=\Big((n+1)\omega-\frac{1}{2}\omega_0\Big)\hbar B_{0n+1}(t)+i\hbar g\sqrt{n+1}B_{0n+1}(t)\Rightarrow$$

$$\Rightarrow\dot{B}_{0n+1}(t)=-\frac{i}{2}(\omega-\omega_0)B_{0n+1}(t)+g\sqrt{n+1}A_{1n}(t)\qquad(18)$$

Now since we are interested for the case of resonance where $\omega=\omega_0$ equations (17) and (18) take the final form:

$$\dot{A}_{1n}(t)=-g\sqrt{n+1}B_{0n+1}(t)\qquad(19)$$

$$\dot{B}_{0n+1}(t) = g\sqrt{n+1}A_{1n}(t) \qquad (20)$$

These equations can be solved if we differentiate (19) with respect to time and substitute in the value of $\dot{B}_{0n+1}(t)$ from (20), and vice versa:

$$\ddot{A}_{1n}(t) = -g^2(n+1)A_{1n}(t) \qquad (21)$$

$$\ddot{B}_{0n+1}(t) = -g^2(n+1)B_{0n+1}(t) \qquad (22)$$

The solutions for equations (21), (22) have the form:

$$A_{1n}(t) = C_1 \cos\left(g\sqrt{n+1}\right)t + C_2 \sin\left(g\sqrt{n+1}\right)t \qquad (23)$$

$$B_{0n+1}(t) = C_3 \cos\left(g\sqrt{n+1}\right)t + C_4 \sin\left(g\sqrt{n+1}\right)t \qquad (24)$$

Now if we put the initial conditions for the state of atom-field $|1\rangle|n\rangle$ at time t=0 (which means that $|A_{1n}|^2 = 1$), we can evaluate the coefficients C_1-C_4. So we can finally find the occupation probabilities for the two states as:

$$|A_{1n}(t)|^2 = \cos^2(g\sqrt{n+1})t \qquad |B_{0n+1}(t)|^2 = \sin^2(g\sqrt{n+1})t \qquad (25)$$

Finally for the case of vacuum inside the cavity (n=0) the probabilities become:

$$|A_{1n}(t)|^2 = \cos^2 gt \qquad |B_{0n+1}(t)|^2 = \sin^2 gt \qquad (26)$$

The interpretation of equations (26) is very astonishing. They imply that an excited atom entering a vacuum cavity (no photons present) can make a transition from upper to lower state emitting a photon. This photon can be reabsorbed by the atom. There is a sinusoidal exchange of the energy between

the atom and the cavity (the so called Rabi oscillations between excited and ground state). This model of spontaneous emission is very different from the well-known exponential decay in free space. In this case the atom interacts with a continuum of modes and not a single mode field. The single mode interaction is the phenomenon predicted by Jaynes-Cummings model and is due to the vacuum fluctuations[24], which are firmly established in the QED theory. The emission of the photon is reversible. This reversibility makes this quantum system a potential candidate for the construction of a quantum gate.

B. IMPLEMENTATION OF A 2-BIT UNIVERSAL GATE

1. Description of the Proposed Apparatus

In 1995 Tycho Sleator and Harald Weinfurter proposed a 2-bit universal gate based on cavity QED techniques.[17] We will refer to these authors as SW. We are now able with the theoretical background presented earlier to describe and discuss this realization of quantum gate.

The proposed implementation involves microwave cavities, Ramsey zones and two-state atoms. The atoms are considered as the carriers of the bits. Their two accessible states are the ground and excited state represented by $|0\rangle$ and $|1\rangle$ respectively. The cavity is either in vacuum state $|0\rangle$ with zero photons present or in state $|1\rangle$ with only one photon present. There are two kinds of interaction between cavity and atoms. When the cavity frequency ω is equal to the frequency ω_0 of atomic transition between excited and ground state, the

cavity is "on resonance" and the interaction of cavity with atoms is described by the Hamiltonian of equation (9) above. It is noted here that in their paper SW present a slightly different Hamiltonian for this interaction. When the cavity frequency is not ω_0, then there are no transitions between excited and ground state for the atom inside the cavity. The Ramsey zones can produce a rotation of the states of atoms in accordance with the frequency and amplitude of the induced field. In the proposed scheme the researchers use Ramsey zones that produce a rotation of π/2 of the spin about the y-axis. The operator for this rotation is given by σ_y which is defined earlier as $\sigma_y = i(\sigma_{12} - \sigma_{21})$.

The interaction of an atom that passes through a Ramsey zone R, the off resonant cavity and a Ramsey zone R^{-1} is given according to SW by the following transformation to its state:

$$U = R^{-1}(e^{i\phi\alpha^{+}\alpha\sigma_{22}})R \qquad (27)$$

where φ is the angle of rotation of the atomic state.

2. Description of a Control-NOT Operation

For the implementation of a control-NOT operation using this scheme, two atoms are required. The first atom is the control bit while the second one is the target bit. A control-NOT operation is characterized by the following truth table:

INPUT BITS		OUTPUT BITS	
CONTROL BIT	TARGET BIT	CONTROL BIT	TARGET BIT
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Table 5.1 Truth Table for Control-NOT operation

When the cavity is on resonance we can transfer quantum states from the atoms to the cavity. We showed in previous section that when an excited two-state atom passes through the on-resonance cavity and there are no photons present (vacuum state) there is a transition of the atom from upper to lower state and the emission of a single photon. This photon is stored in the cavity long enough to interact with the next atom that passes. If the atom is not excited and passes through the on-resonance cavity in the vacuum state, nothing happens. So we see that the state of the first atom which is the control bit passes to the cavity. The cavity is always in the beginning in vacuum state $|0\rangle$. If the atom is in state $|0\rangle$ the cavity remains in that state. If the atom is in state $|1\rangle$, this state is transferred to the cavity as described above and cavity is then in state $|1\rangle$.

The second atom passes through the Ramsey zones and the off resonant cavity. The state of this atom is transformed in accordance with equation (23) above. When the cavity is in state $|1\rangle$ the state of the atom undergoes a rotation. When the cavity is in state $|0\rangle$ the state of the atom does not change.

The control bit leaves the cavity in state $|0\rangle$. When the operation is complete the gate is ready to operate again.

3. Discussion

The above proposal for a quantum gate is feasible with current technology, even though it is far from being miniaturized. The transfer of the

state of the control bit to the cavity is predicted by the Jaynes-Cummings model as noted earlier. Experiments in 1987 have demonstrated the predictions of the theory.[25] The cavity operated at 21.6 GHz with a temperature of 2.5K. The atoms used were rubidium excited by laser radiation to the $63P_{3/2}$ state. The transition was made inside the cavity to the $61D_{5/2}$ state. The flux of the atoms that were crossing the cavity was low and the cavity had ample time to "relax."

The photon released by an excited atom is stored, as aforementioned, long enough inside the cavity, thus allowing interaction with the next passing atom. It should be noted that we have not included in our treatment the cavity decay, which plays a very important role for the time that the photon will be present in the cavity. The cavity decay is one of the decoherence mechanisms for this implementation, which will be discussed further in the next Chapter. The decoherence problems encountered with this specific realization have not been addressed, as far as we know, and they must be studied in order to calculate the actual computation time of the gate.

Another fine point is that the cavity has to operate in very low temperatures to avoid the existence of thermal photons. The presence of thermal photons in the cavity affects the evolution of the system. There is not a sinusoidal exchange of energy between atom and photon and so we now show the Rabi oscillations wash out.[24,25]

We know that in thermal equilibrium the probability of a photon to be in the nth excited state is given by the Boltzmann factor:

$$P_n = \frac{e^{-E_n/k_BT}}{\sum_{n=0}^{\infty} e^{-E_n/k_BT}} \tag{28}$$

Since the energy takes discrete values according to $E_n = (n+\frac{1}{2})\hbar\omega$, we can write equation (28) as:

$$P_n = \frac{e^{-n\hbar\omega/k_BT} e^{-\hbar\omega/2k_BT}}{e^{-\hbar\omega/2k_BT}\sum_{n=0}^{\infty} e^{-n\hbar\omega/k_BT}} = \frac{e^{-n\hbar\omega/k_BT}}{\sum_{n=0}^{\infty} e^{-n\hbar\omega/k_BT}} \tag{29}$$

The denominator is a geometric series with sum:

$$\sum_{n=0}^{\infty} e^{-n\hbar\omega/k_BT} = \sum_{n=0}^{\infty}\left(e^{-\hbar\omega/k_BT}\right)^n = \frac{1}{1-e^{-\hbar\omega/k_BT}} \tag{30}$$

and equation (29) can be written as:

$$P_n = e^{-n\hbar\omega/k_BT}\left(1-e^{-\hbar\omega/k_BT}\right) \tag{31}$$

So now we can calculate the mean number of photons $\bar{n}$:

$$\bar{n} = \sum_{n=0}^{\infty} nP_n = \left(1-e^{-\hbar\omega/k_BT}\right)\sum_{n=0}^{\infty} ne^{-n\hbar\omega/k_BT} = \left(1-e^{-\hbar\omega/k_BT}\right)e^{-\hbar\omega/k_BT}\frac{\partial}{\partial\left(e^{-\hbar\omega/k_BT}\right)}\sum_{n=0}^{\infty}\left(e^{-\hbar\omega/k_BT}\right)^n =$$

$$= -\left(1-e^{-\hbar\omega/k_BT}\right)e^{-\hbar\omega/k_BT}\frac{1}{\left(1-e^{-\hbar\omega/k_BT}\right)^2} = \frac{-e^{-\hbar\omega/k_BT}}{e^{-\hbar\omega/k_BT}\left(1-e^{\hbar\omega/k_BT}\right)} \Rightarrow$$

$$\Rightarrow \bar{n} = \frac{1}{e^{\hbar\omega/k_BT}-1} \tag{32}$$

And then the probability of having n photons present when the mean number is $\bar{n}$ is given by:

$$P_n = \left(\frac{\bar{n}}{\bar{n}+1}\right)^n \left(1-\frac{\bar{n}}{\bar{n}+1}\right) = \left(\frac{\bar{n}}{\bar{n}+1}\right)^n \left(\frac{\bar{n}+1-\bar{n}}{\bar{n}+1}\right) = \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} \qquad (33)$$

Now we calculate the expectation value of photons as given by the Jaynes-Cummings model, using the wave function introduced in equation (10):

$$\langle n(t)\rangle = \langle \psi | \alpha^+ \alpha | \psi \rangle = \langle \left(A_{1n}(t)\langle n|\langle 1| + B_{0n+1}(t)\langle n+1|\langle 0| \right) \alpha^+ \alpha \left(A_{1n}(t)|1\rangle|n\rangle + B_{0n+1}(t)|0\rangle|n+1\rangle \right) \rangle \Rightarrow$$

$$\Rightarrow \langle n(t)\rangle = n|A_{1n}|^2 + (n+1)|B_{0n+1}|^2 \qquad (34)$$

Using the values calculated for $|A_{1n}|^2$ and $|B_{0n+1}|^2$ from equation (26) :

$$\Rightarrow \langle n(t)\rangle = n\cos^2(g\sqrt{n+1})t + (n+1)\sin^2(g\sqrt{n+1})t = n + \sin^2(g\sqrt{n+1})t$$

Since $\bar{n} = \sum_{n=0}^{\infty} nP_n$ we can obtain for our model:

$$\langle n(t)\rangle = \sum_{n=0}^{\infty} P_n[n + \sin^2(g\sqrt{n+1})t] = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}}[n + \sin^2(g\sqrt{n+1})t] \Rightarrow$$

$$\Rightarrow \langle n(t)\rangle = \bar{n} + \left(\frac{1}{\bar{n}+1}\right)\sum_{n=0}^{\infty}\left(\frac{\bar{n}}{\bar{n}+1}\right)^n \sin^2(g\sqrt{n+1})t \qquad (35)$$

Now we can plot $\langle n(t)\rangle - \bar{n}$ to see the effect in the evolution of the Rabi oscillations of a thermal filed with a mean number of $\bar{n}$ photons present in the cavity. Figure 5.1 below is a plot for $\bar{n} = 2$, $\bar{n} = 10$ and $\bar{n} = 100$. For the time t we have introduced the dimensionless quantity $T = g\bar{n}$, with $\bar{n} = 1$ for all plots.

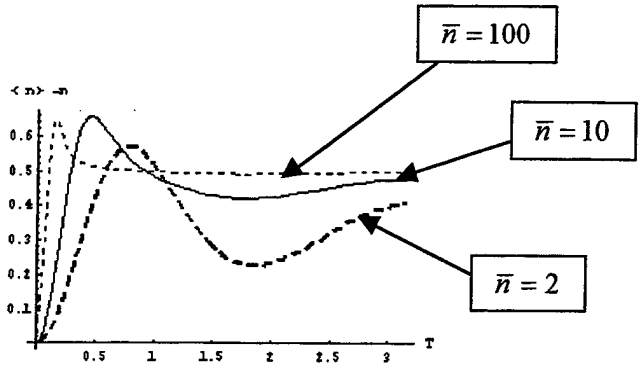

Figure 5.1 plot of $\langle n(t)\rangle - \overline{n}$

We see from the above figure that the Rabi oscillations wash out for a thermal field. Also we see that the damping of the oscillations is more rapid when the mean number of photons is bigger, i.e. when the temperature is higher. That is the reason we need very low temperatures to implement this gate.

Even though the first results from such an implementation look promising, we believe that it is not feasible, at least with current technology, to build a quantum network with such gates. The most difficult obstacle is to maintain the required coherence between all cavities used for the gates. Another serious problem is the fact that all the cavities have to be cooled in very low temperature.

In any case this proposal is a first step towards the construction of quantum networks. The basic advantage is that it uses 2-bit gates, which are more easily implemented instead of 3-bit. Also the system can be used to carry out more experiments.

A slightly different approach had been presented[26] by a research group of University of Innsbruck. Their scheme is also based on cavity QED and the Jaynes-Cummings model. They utilize a set of N atoms fixed inside a high Q cavity. The interaction of each atom with the single mode field of the cavity allows the communication between them. Laser beams are also utilized to interact individually with each atom, thus allowing the performance of continuous operations between various qubits and the construction of a quantum network. The group presented this scheme in a paper published in 1995 and they also had some first calculations for the effect of decoherence along with a possible solution.

There are also proposals for 3-bit gates using cavity QED techniques.[8] They are based in the interaction of a single mode field with three-state atoms. The Hamiltonian used to describe this interaction with the on resonant cavity is the same as the one in equation (2). But the implementation of the gate is different from the one described above. It is based on the principle of "dark states". Some researchers believe that this proposal will experience less decoherence problems than the 2-bit gate.

VI. DECOHERENCE AND CAVITY QED COMPUTERS

A. GENERAL

There are a numerous obstacles that need to be overcome before quantum computers can be successfully implemented. We will not deal with feasibility questions such as whether the implementation is possible with current or future technology, since we believe there are presently many theoretical questions that remain unanswered.

In the previous Chapters we described the elements of quantum computers and their possible realization making very naive assumptions. All the systems used were considered "ideal". Thus, all the operations were ideal, something that will never happen in reality.

We can categorize the errors encountered in a quantum computer as two general types.[12] The first type of errors can be called internal errors. They arise due to imperfections in the original design of the system and in the initial data. The design of the system consists of the quantum system implemented for the gates and the measurement techniques for the output. The general belief a few years ago that there were no ways to overcome these problems has been proved false. Quantum error correction methods along with fault-tolerant design of quantum systems have been developed, demonstrating that an actual quantum computation could be performed in the future. It is beyond the scope of

this thesis to describe and discuss further these fields but we must emphasize their importance for the future prospects of quantum computation.

The second category is the so called external errors. This is the most difficult obstacle to overcome and may be the one that will make actual quantum computing impossible. This has to do with the fragility of quantum information, which is a consequence of the decoherence appearing in the evolution of a quantum system. The notion of decoherence and its effect on quantum computation is the subject of this chapter. The study of decoherence is very difficult. First we will give a general definition of decoherence. Then we will present some intuitive considerations in order to understand the phenomenon and identify its origin. We will continue presenting some of the possible models required to study the phenomenon quantitatively and finally we will discuss the effects of decoherence on cavity QED based quantum gates.

B. DECOHERENCE

1. General Notion and Meaning of Decoherence

As was noted earlier (Chapter II) the reversible unitary evolution of a quantum system is necessary for the performance of a successful computation. In order to achieve this we must ensure that the evolved system is closed. That is the system must not interact with the environment. The interaction with the environment has as a result the addition of more degrees of freedom, that are not included in the Hamiltonian which describes the closed system. Then the

evolution of the system is not the one predicted by the original Hamiltonian and any quantum information contained in the system is gradually lost. This process is called decoherence.

The phenomenon of decoherence is so efficient that is very difficult to observe it experimentally. Some superconducting systems were recently developed for this purpose and they demonstrated the phenomenon.[27]

As noted by Roland Omnès[27] the existence of decoherence for macroscopic objects is due to their large Hilbert space and their crowded energy spectrum. According to perturbation theory the wave function changes under the influence of any small perturbation. This change is inversely proportional to the difference of the unperturbed energy levels. The closeness of the energy levels in a macroscopic object results in very small differences between them, which consequently has as an effect an enormous increase of any small perturbation. The effect in microscopic objects is not so efficient or so rapidly developed but it still exists. Microscopic systems do not have such enormous Hilbert spaces but decoherence appears due to their coupling with the environment which is considered a system with an enormous Hilbert space.

There are various models that give quantitative results for certain systems and with specific assumptions. However, a general model or theory does not exist due to the difficulty of the problem.

2. Physical Meaning of Density Matrix Elements

In Chapter II we introduced the density operator and its matrix representation. We will now present the meaning of the diagonal and non-diagonal matrix elements ρ_{nn} and ρ_{nm} respectively for a statistical mixture of states.[6]

According to equation (20) of Chapter II $\rho(t) = \sum_k p_k \rho_k(t)$. From the definition of density operator we can write:

$$\rho_{nn} = \sum_k p_k (\rho_k)_{nn} \tag{1}$$

Also we have that $c_n^k = \langle u_n | \psi_k \rangle$ and so we can write:

$$|c_n^k|^2 = \langle u_n | \psi_k \rangle \langle \psi_k | u_n \rangle \tag{2}$$

Then we can rewrite (1) using (2) and the fact that $\rho_k = |\psi_k\rangle\langle\psi_k|$ as:

$$\rho_{nn} = \sum_k p_k |c_n^k|^2 \tag{3}$$

with $|c_n^k|^2$ zero or a positive real number. The ρ_{nn} is zero only when all the coefficients $|c_n^k|^2$ are equal to zero. These coefficients represent the average probability of finding the system in the state $|u_n\rangle$. The probability is defined as average due to the fact that the state is undetermined before the measurement. If we perform the same measurement N times with the same initial conditions we

will find the system $N\rho_{nn}$ times in the state $|u_n\rangle$. For this reason ρ_{nn} is called the population of state $|u_n\rangle$.[6]

For the non-diagonal elements of the matrix we can follow the same derivation as above. We have that:

$$\rho_{nm} = \sum_k p_k (\rho_k)_{nm} \tag{4}$$

Also we can write:

$$c_n^k c_m^{k*} = \langle u_n | \psi_k \rangle \langle \psi_k | u_m \rangle \tag{5}$$

And we finally have using again the fact that $\rho_k = |\psi_k\rangle\langle\psi_k|$:

$$\rho_{nm} = \sum_k p_k c_n^k c_m^{k*} \tag{6}$$

These elements express the interference between the states $|u_n\rangle$ and $|u_m\rangle$, when the state $|\psi_k\rangle$ is a linear superposition of these states. From its definition we see that ρ_{nm} is the sum of complex numbers. Thus, ρ_{nm} can be zero even if none of the products $c_n^k c_m^{k*}$ is zero. If ρ_{nm} is not zero then we can infer that a certain coherence exists between the states $|u_n\rangle$ and $|u_m\rangle$. If ρ_{nm} equals zero, however, then this coherence does not exist. That's why the off-diagonal elements are called coherences.[6]

3. Reduced Density Matrix

Now we are going to assume that a quantum system (denoted as system A) and the environment (denoted as system E) comprises a new "total" system.

As was mentioned in Chapter II the Hilbert space for the total system will be the tensor product of the individual Hilbert spaces H_A and H_E. The density operator ρ of the total system is defined for the total Hilbert space. The trace of this operator is defined as:

$$Tr\rho = \sum_n \sum_m \left(\langle u_n(A) | \langle u_m(E) | \right) \rho \left(| u_n(A) \rangle | u_m(E) \rangle \right) \qquad (7)$$

Then we can define a new operator ρ_A that will operate only on the H_A space. This operator can be constructed by performing a partial trace on E:

$$\rho_A = Tr_E \rho \qquad (8)$$

The matrix elements for ρ_A are:

$$\langle u_n(A) | \rho_A | u_{n'}(A) \rangle = \sum_m \left(\langle u_n(A) | \langle u_m(E) | \right) \rho \left(| u_{n'}(A) \rangle | u_m(E) \rangle \right) \qquad (9)$$

Similarly we can define the operator $\rho_E = Tr_A \rho$ and its matrix elements are:

$$\langle u_m(E) | \rho_B | u_{m'}(E) \rangle = \sum_n \left(\langle u_n(A) | \langle u_m(E) | \right) \rho \left(| u_n(A) \rangle | u_{m'}(E) \rangle \right) \qquad (10)$$

These two operators are called reduced density operators. Their trace is also equal to 1, like the ρ operator. From equations (9) and (10) we can also see that:

$$Tr\rho = Tr_A(Tr_E \rho) = Tr_E(Tr_A \rho) \qquad (11)$$

The reduced operators allow us to make predictions about the possible outcomes of measurements for system A or system E alone. The diagonal and

non-diagonal elements of the reduced operator matrix have similar definitions and properties as the ones discussed above (equations 3-6) for the operator ρ.

This means that the non-diagonal terms of the reduced density operator for the system represent the interference between various states of the system.

In the case where we can identify the interaction Hamiltonian between the quantum system and the environment, it is shown[27-29] that the system density matrix becomes diagonal (i.e. the non-diagonal terms have vanished) in the basis defined by the interaction Hamiltonian. This is the effect of decoherence. So if someone wants to find quantitative results for the decoherence of a system he must find a way to describe the time evolution of the reduced density matrix $\rho_A = Tr_E \rho$.

However this is not easy. Even though we can describe the evolution of the total system (A+E) by equation (18) of Chapter II ($i\hbar \frac{d}{dt}\rho(t) = [H(t), \rho(t)]$), it is very difficult (sometimes almost impossible)[6] to find a similar equation for the reduced density operator of the system A. This is the fact that makes the study of decoherence very difficult.

C. DECOHERENCE IN CAVITY QED BASED GATES

For the cavity QED based gate that was described in Chapter V there are two sources of decoherence. The spontaneous emission by the transition of the atom from excited to ground state and the cavity decay (loss of the photon). Both these mechanisms are damping mechanisms. The Hamiltonian we derived in the

previous Chapters did not include these damping mechanisms. It was an "ideal" Hamiltonian. But in an actual gate the coupling with the environment is inevitable. Thus, the actual performed computation will be different from what the ideal Hamiltonian suggests and may include errors. Thus, we have to find quantitative results for the effects of decoherence. This way we will know the actual evolution of the gate and we can develop methods to compensate for any possible errors.

As was noted earlier, in order to find quantitative results for decoherence effects, we must find an expression for the evolution of the reduced density operator of the gate. The most widely used method is by means of the master equation.[26,28,29] There are two different ways to implement the decay of the system in master equations. The first one is in the case where the decay of the system is not observed (*a priori dynamics*).[26,30] The second one is in the case where there is implemented a continuous photodection process for the photons emitted spontaneously by excited atoms and for photons coming from the cavity decay. This is called *a posteriori dynamics*.[26,30]

The basic formalism of quantum theory for such photodetection processes can be found in published papers[30-32] and a few advanced textbooks. The implementation of this method in a quantum computer based on cavity QED techniques has been presented by a research group of University of Innsbruck.[26] According to their results it is possible to predict the decoherence effects and compensate them, thus making feasible an actual computation. Also they argue

that this method can be used to derive quantitative decoherence results for any quantum gate based in cavity QED techniques. This is true since the dumping mechanisms for all these quantum gates are the same.

However, if it is implemented in the scheme described in Chapter V, we believe that it will give results for a stand-alone quantum gate. A quantum computer constructed by such gates will experience more problems since there are more possible decoherence mechanisms involved, due to the required "wiring" between gates.

Finally, we note that even if we can't find ways to compensate for the decoherence, the study can give us an estimation for the decoherence time which in fact is the the time limitation for the performance of the quantum gate.

VII. POSSIBLE MILITARY APPLICATIONS

It has already been mentioned that quantum computation is a new field that has been developed for only a few years. One of the weak points of the field is the difficulty of the notion that quantum mechanics and computer science can be combined. As was noted earlier the two fields have been developed independently for over fifty years. There is a significant intellectual gap between the theoretical scientists of these fields, which results in the difficulty to understand the fundamental aspects of each other.

This fact, along with the obstacles encountered so far for the implementation of a quantum computer, are the primary reasons for the absence of proposed applications.

The only application that has been proposed until now and could have a military interest, as far as we know, is Shor's algorithm. The efficiency of this algorithm to perform factorization of large numbers could undermine the security of computer systems worldwide. Thus, a government that could build a quantum computer to run this algorithm would gain a significant advantage over the rest of the world. Quantum computers could play the role of first-class weapons in a possible future "information war".

However, this is not the only military application of quantum computation. Someone could think of a variety of applications only by reading the article of Richard Feynman[1], which was the starting point for quantum computation.

According to Feynman a classical computer can never simulate a quantum system. The only way to accomplish this is by quantum computers. David Deutsch had a similar approach to the problem and he also made a very definite statement for the capabilities of quantum computer.[3] They can perfectly simulate every finitely realizable physical system.

Starting from this fact we could think some of the possible systems that could be simulated and have a military interest.

One of the most important applications could be the design and test of nuclear weapons. There is already a program called Accelerated Strategic Computing Initiative (ASCI) sponsored by the Department of Energy.[7] The primary purpose of this program is to establish a capability for designing and testing nuclear weapons solely based in computer simulations. The success of this ambitious program is based on the fact that a conventional supercomputer could perform all the available calculations. Even though we don't know the aspects of the program the theoretical question raised by Feynman and Deutsch will remain unanswered until the completion of the project. An alternative approach could be the usage of quantum computers for performing the required simulations.

Similarly the quantum computers could perform simulations for the testing of future aircraft, missiles and other weapon systems. Even though it is premature to discuss the construction of quantum computers, the effects of their usage in such applications would have tremendous impact in our society. The

cost for the development of new weapons could be reduced dramatically (assuming that the cost for the construction of a quantum computer would not be very high). A more significant consequence would be the elimination of actual tests for the capabilities of these weapons. This would have as a result the difficulty to identify the technology level of an enemy by observing the conducted tests. Thus, quantum computers could be a new threat in the long run for the security of every nation. Fortunately or unfortunately, depending on someone's point of view, all these are currently science fiction scenarios and they may stay this way forever.

Another possible application of quantum computers is computer vision. Computer vision[33] is a field of artificial intelligence that describes the understanding of the structure and properties of the three dimensional world from its two dimensional images. The most important fields of computer vision are image processing and pattern recognition. Since images contain an enormous amount of information most of the currently developed techniques utilize methods for data reduction. This is accomplished by edge detection and segmentation algorithms. It is inevitable that in the process some information of the original image can be lost. The problem becomes more complicated in the case of a passive observer[33] (an observer that has no control over the image acquisition process). Quantum computers could analyze the enormous amount of data, in very short times, due to their parallelism capabilities. Most of the future unmanned vehicles will rely more and more on computer vision for their

navigation and the successful accomplishment of their mission. Thus, we believe that a further study is required to determine and analyze the implementation of quantum computers and algorithms in computer vision techniques.

VIII. DISCUSSION-FUTURE PROSPECTS OF QUANTUM COMPUTATION

In the previous chapters we presented some of the aspects that make quantum computers a powerful tool and give them the theoretical ability to solve problems that current conventional computers cannot. The theoretical advancements in quantum theory and the technological breakthrough in quantum devices over the last decade give the chance to actually build some fundamental gates that can perform a computation. It is noted that these gates are far from being a whole computer system that will operate and solve actual problems.

Also, even if we manage to construct an actual quantum computer, in the future it will not be the one that will replace the machines we are using today. Furthermore, it won't be a low priced desk-size machine, like the conventional ones that almost everyone can buy and use.

There are many obstacles that need to be overcome before one can envision the implementation of quantum computers, the most important being the phenomenon of decoherence. For the rest of the problems as are described in published papers and articles we have a slightly different opinion.

We won't argue that difficulties regarding the cost and size of proposed machines can force the research community to abandon the effort. The evolution of current conventional machines is an example. The continuous development of miniaturization techniques transformed the huge, slow processing machines of

1950 to today's mini, ultra fast supercomputers. There is no reason (at least a theoretical one) that this could not happen for the proposed schemes of quantum computers.

Even if someone suggests that we could never achieve such miniaturization, quantum computers could be built by large companies or governments that are interested to solve specific problems, regardless the required cost and manpower.

We believe that quantum computation is an important development and its implications in physics and computer science are just beginning to be apparent. The field has been emerging for only a few years. Thus, a definite assessment for the future prospects cannot be made. In any case we would like to point out a few things regarding the current status of the field.

The absence of proposed applications is a weak point of the field. The identification of additional possible applications will attract the investment of more resources, which are critical for the continuation of research.

The proposed quantum algorithms are few and there is an urgent need for the development of more algorithms.

The theoretical research should focus more on the decoherence problems encountered in every proposed realization. A possible solution could be found by the usage of quantum error correction codes[8] and by the design of fault tolerant quantum gates[8].

The construction of an actual quantum computer depends on technological breakthroughs in quantum devices. However, the miniaturization of quantum gates is not a critical problem, at least for the moment, as was already argued.

This thesis was a first approach to describe the fundamental elements of quantum computation and their implementation by means of cavity QED techniques. It is far from being an elaborate treatment for quantum computers. There are as aforementioned more fundamental elements and proposed realizations that need to be presented and analyzed.

Quantum computation is a vast subject involving a lot of research in the forefront of theoretical physics. Thus, we believe that a research program should be adopted in order to establish a firm result for the feasibility of quantum computation.

The major milestones of such a theoretical program could be the following:

1. Evaluation of all proposed realizations and identification of the most promising one.

2. Further analysis of this realization by identifying the actual computation times due to technology limitations and decoherence effects.

3. Development and implementation of quantum error correction codes to achieve the desired computational times.

4. Development of appropriate quantum algorithms, which will test the computing performance.

The success of such a program cannot be guaranteed but nevertheless we believe its adoption is worthy.

Even if quantum computation fails, the insight we have already gained for quantum systems is very important. We dealt with theoretical aspects that maybe we would never encounter or maybe only a few would have. The only fact that everybody seems to agree is that we need more years of development to reach at a point that we can definitely evaluate the concept of quantum computers. And until then we are sure that more profound developments towards understanding nature itself will be made. After all that is the ultimate goal of physics.

APPENDIX A DERIVATION OF RELATION $\int d^3r[\nabla \times \mathbf{A}(\mathbf{r})]^2 = k^2 \int d^3r\mathbf{A}(\mathbf{r})^2$

We want to prove that:

$$\int d^3r[\nabla \times \mathbf{A}(\mathbf{r})]^2 = k^2 \int d^3r\mathbf{A}(\mathbf{r})^2 \qquad (1)$$

We will use two vector identities:

$$\nabla \cdot (\mathbf{F} \times \mathbf{G}) = \mathbf{G} \cdot \nabla \times \mathbf{F} - \mathbf{F} \cdot \nabla \times \mathbf{G} \qquad (2)$$

$$\nabla \times (\nabla \times \mathbf{A}) = \nabla(\nabla \cdot \mathbf{A}) - \nabla^2\mathbf{A} \qquad (3)$$

Then we can write the right hand side of equation (1) using the identity (2) with $\mathbf{G} = \nabla \times \mathbf{A}$ and $\mathbf{F} = \mathbf{A}$:

$$(\nabla \times \mathbf{A})^2 = (\nabla \times \mathbf{A}) \cdot (\nabla \times \mathbf{A}) = \nabla \cdot (\mathbf{A} \times \nabla \times \mathbf{A}) + \mathbf{A} \cdot \nabla \times (\nabla \times \mathbf{A}) =$$

$$= \nabla(\mathbf{A} \times \nabla \times \mathbf{A}) + \mathbf{A}\left[\nabla \cdot (\nabla \cdot \mathbf{A}) - \nabla^2\mathbf{A}\right] = \nabla \cdot (\mathbf{A} \times \nabla \times \mathbf{A}) - \mathbf{A}\nabla^2\mathbf{A} \qquad (4)$$

We will also use the fact that we are working in the Coulomb gauge, in which the vector potential A satisfies the following relation:

$$\nabla \cdot \mathbf{A} = \mathbf{0} \qquad (5)$$

and Helmholtz's equation:

$$\nabla^2\mathbf{A} + k^2\mathbf{A} = \mathbf{0} \qquad (6)$$

Then equation (4) can be written using (5) and (6) as:

$$(\nabla \times \mathbf{A})^2 = \nabla \cdot (\mathbf{A} \times \nabla \times \mathbf{A}) + k^2\mathbf{A} \qquad (7)$$

So now the integral of equation (1) can be written using (7) and the divergence theorem as:

$$\int d^3r[\nabla \times \mathbf{A}(\mathbf{r})]^2 = \int d^3r \nabla \cdot (\mathbf{A} \times \nabla \times \mathbf{A}) + \int d^3r k^2 \mathbf{A}(\mathbf{r})^2 =$$

$$= \oint dS \cdot \hat{\mathbf{n}} \cdot \mathbf{A} \times (\nabla \times \mathbf{A}) + \int d^3r k^2 \mathbf{A}(\mathbf{r})^2 = k^2 \int d^3r \mathbf{A}(\mathbf{r})^2 \qquad (8)$$

The first integral in above equation (8) is a surface integral and vanishes due to the periodic boundary conditions imposed on vector potential A. Thus, we finally have the required equation:

$$\int d^3r[\nabla \times \mathbf{A}(\mathbf{r})]^2 = k^2 \int d^3r \mathbf{A}(\mathbf{r})^2$$

APPENDIX B DERIVATION OF EQUATION (46) OF CHAPTER IV

We start from Helmholtz's theorem: Any vector field **F** can be expressed into a transverse and longitudinal part with the following properties:

$$\nabla \cdot \mathbf{F}^{\perp}(\mathbf{r}) = 0 \qquad \nabla \times \mathbf{F}^{//}(\mathbf{r}) = \mathbf{0} \qquad (1)$$

Now if we apply this theorem for the **E** field and we use the fact of the Coulomb gauge along with the vector identity $\nabla \times \nabla\phi = 0$, we can see that the electric field vector $\vec{E} = -\frac{1}{c}\frac{\partial \vec{A}}{\partial t} - \nabla\varphi$, can be decomposed in the two parts as:

$$\mathbf{E}^{\perp} = -\frac{1}{c}\frac{\partial \mathbf{A}}{\partial t} \text{ and } \mathbf{E}^{//} = -\nabla\phi \qquad (2)$$

Then we can write for the **E** field contribution to the total field energy:

$$\int d^3r\mathbf{E}^2 = \int d^3r(\mathbf{E}^{\perp 2} + \mathbf{E}^{//2} + 2\mathbf{E}^{\perp}\mathbf{E}^{//}) \qquad (3)$$

Now we have that:

$$\int d^3r\mathbf{E}^{\perp} \cdot \mathbf{E}^{//} = 0 \quad \int d^3r\mathbf{E}^{//2} = \int d^3r(\nabla\phi)^2 \qquad (4)$$

Using the vector identity $\nabla(\phi\psi) = (\nabla\phi)\psi + \phi\nabla\psi$ we have that:

$$\nabla(\phi\nabla\phi) = (\nabla\phi)(\nabla\phi) + \phi\nabla \cdot \nabla\phi \Rightarrow (\nabla\phi)^2 = \nabla(\phi\nabla\phi) - \phi\nabla^2\phi \qquad (5)$$

Now using equation (5) the second equation from (4) can be written as:

$$\int d^3r\mathbf{E}^{//2} = \int d^3r(\nabla\phi)^2 = \int d^3r\nabla(\phi\nabla\phi) - \int d^3r\phi\nabla^2\phi \qquad (6)$$

For the first term in equation (6) we can use Gauss theorem to convert the volume integral to a surface integral and then let the surface extend to infinity, thus making the value of the integral zero:

$$\int d^3r\nabla(\phi\nabla\phi) = -\oint_S ds\phi\mathbf{E} = \mathbf{0} \qquad (7)$$

Now for the second term of equation (6) we have that $\nabla^2\phi = -4\pi\rho$ and so we can write it as:

$$4\pi\int d^3r\rho\phi \qquad (8)$$

The complete Hamiltonian for a system of n charged particles and the electromagnetic field can thus be written:

$$H = \sum_{i=1}^{n}\frac{1}{2m_i}\left(\mathbf{p}_i - \frac{q_i}{c}\mathbf{A}_i\right)^2 + \frac{4\pi}{8\pi}\int d^3r\rho(\mathbf{r})\phi(\mathbf{r}) + \frac{1}{8\pi}\int d^3r\left(\mathbf{E}^{\perp 2} + \mathbf{B}^2\right) \qquad (9)$$

So now since we do not have a continuous charge distribution but particles at specific positions we want to find an equivalent expression for the second term of equation (9) above.

We know that the potential φ that one of the charged particles "sees" is produced by the rest of the particles (n-1) and can be expressed[29] as:

$$\phi(\mathbf{r}_i) = \frac{1}{4\pi}\sum_{j=1}^{n-1}\frac{q_j}{|\mathbf{r}_i - \mathbf{r}_j|} \qquad (10)$$

Also we know that the product of scalar potential and the charge of a particle is the potential energy. So we can write for the potential energy of a charge q_i:

$$V_i = \frac{q_i}{4\pi} \sum_{j=1}^{n-1} \frac{q_j}{|\mathbf{r_i} - \mathbf{r_j}|} \tag{11}$$

Then the total potential energy of all particles is:

$$V = \frac{1}{4\pi} \sum_{i=1}^{n} \sum_{i>j} \frac{q_i q_j}{|\mathbf{r_i} - \mathbf{r_j}|} \tag{12}$$

Equation (12) can be written in a different form if we sum over all i, j and we divide by a factor of 2 to avoid double counting:

$$V = \frac{1}{8\pi} \sum_{i} \sum_{j} \frac{q_i q_j}{|\mathbf{r_i} - \mathbf{r_j}|} \tag{13}$$

We also know that a discrete set of point charges can be written as a charge density using delta functions:[29]

$$\rho(\mathbf{r}) = \sum_{i=1}^{n} q_i \delta^3(\mathbf{r} - \mathbf{r_i}) \tag{14}$$

If we substitute the above expression in the second term of equation (9) and use the definition of delta function we get the same expression of equation (13).

Now in the case where all particles are fixed in position except the one that we want to know its evolution, then equation (13) represents the potential energy V(**r**) for the moving particle due to the other fixed particles[21,29]. This potential energy can be written as:

$$V(\mathbf{r}) = e\phi(\mathbf{r}) \tag{15}$$

where we have assumed that the particle has charge q=e and the potential $\phi(\mathbf{r})$ is known. Then the Hamiltonian for the particle we are interested takes the final form:

$$H = \frac{1}{2m}\left(\mathbf{p} - \frac{e}{c}\mathbf{A}\right)^2 + e\phi + \frac{1}{8\pi}\int d^3r\left(\mathbf{E}^{\perp 2} + \mathbf{B}^2\right) \qquad (16)$$

This is equation (46) of Chapter IV.

APPENDIX C PROPERTIES OF TWO-STATE OPERATORS

We show that the two-state operators $\sigma_x, \sigma_y, \sigma_z$ satisfy the Pauli algebra for spin-1/2 particle. We use the definitions:

$$\sigma_x = \sigma_{01} + \sigma_{10}$$

$$\sigma_y = i(\sigma_{01} - \sigma_{10})$$

$$\sigma_z \equiv \sigma_{11} - \sigma_{00}$$

Then we have:

$$[\sigma_x, \sigma_y] = \sigma_x\sigma_y - \sigma_y\sigma_x = i(\sigma_{01} + \sigma_{10})(\sigma_{01} - \sigma_{10}) - i(\sigma_{01} - \sigma_{10})(\sigma_{01} + \sigma_{10}) =$$

$$= i(-\sigma_{00} + \sigma_{11}) - i(\sigma_{00} - \sigma_{11}) = i\sigma_z + i\sigma_z = 2i\sigma_z \qquad (1)$$

Similar we can find that:

$$[\sigma_y, \sigma_z] = 2i\sigma_x \qquad (2)$$

$$[\sigma_z, \sigma_x] = 2i\sigma_y \qquad (3)$$

Also, since we have defined that $\sigma_{00} + \sigma_{11} = 1$,we have the following properties:

$$\sigma_x^2 = (\sigma_{01} + \sigma_{10})(\sigma_{01} + \sigma_{10}) = \sigma_{00} + \sigma_{11} = 1 \qquad (4)$$

Similar we can show that:

$$\sigma_y^2 = \sigma_z^2 = 1 \qquad (5)$$

Also we have that:

$$\sigma_z|0\rangle = (\sigma_{11} - \sigma_{00})|0\rangle = \sigma_{10}\sigma_{01}|0\rangle - \sigma_{01}\sigma_{10}|0\rangle = \sigma_{10}0 - \sigma_{01}|1\rangle = -|0\rangle \qquad (6)$$

Similar we can find that:

$$\sigma_z|1\rangle = (\sigma_{11} - \sigma_{00})|1\rangle = \sigma_{10}\sigma_{01}|1\rangle - \sigma_{01}\sigma_{10}|1\rangle = \sigma_{10}|0\rangle - \sigma_{01}0 = |1\rangle \qquad (7)$$

LIST OF REFERENCES

1. Richard P. Feynman, Int. J. Theor. Physics, 21, 467 (1982).
2. Richard P. Feynman, Optical News, February 1982.
3. David Deutsch, Proc. R. Soc. London A 400,97 (1985).
4. David P. DiVincenzo, Quantum Computation, Science Vol. 270 13 October 1995.
5. P.W. Shor, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), p. 124 (1994).
6. Claude Cohen-Tannoudgi, Bernard Diu, Franck Laloë, Quantum Mechanics John Wiley&Sons, (1997).
7. Gerald J. Milburn, The Feynman Processor, Perseus Books (1998).
8. Hoi-Kwong Lo, S.Popescu, T. Spiller Introduction to Quantum Computation and Information, World Scientific, (1998).
9. A. Einstein, B. Podolsky and N. Rosen, Physical Review 47, 777 (1935).
10. E. Schrödinger, Proc. Camb. Phil. Soc. 31,555 (1935)
11. Charles H. Bennet, Quantum Information and Computation, Physics today, October 1995.
12. Colin P. Williams, Scott H. Clearwater, Explorations in Quantum Computing Springer-Verlag, (1998).

13. S. Raimes, Many Electron Theory, North Holland Publishing Company, (1972).

14. D.Deutsch, Proc. R. Soc. London A 425,73 (1989).

15. T. Toffoli, Math Systems Theory 14,13 (1981).

16. E. Fredkin and T. Toffoli, Int. J. Theor. Physics,21,219 (1982)

17. Tycho Sleator and Harald Weinfurter, Physical Review Letters Vol. 74, 4087 (1995).

18. L.K. Grover, Physical Review Letters, 79,325 (1997).

19. J.I. Cirac and P.Zoller, Physical Review Letters Vol.74, 4091 (1995).

20. C. Monroe et. al. Physical Review Letters Vol.75,4714 (1995).

21. Peter W. Milloni The Quantum Vacuum An Introduction to Quantum Electrodynamics, Academic Press, (1994).

22. Rodney Loudon The Quantum Theory of Light Oxford University Press, (1983).

23. Stephen Gasiorowicz, Quantum Physics John Wiley&Sons, (1995).

24. P. Meystre, M. Sargent III, Elements of Quantum Optics Springer-Verlag, (1990).

25. Peter W. Milloni and Surendra Singh in Advances in Atomic, Molecular and Optical Physics, Vol.28, Academic Press (1990).

26. T.Pellizari, S.A. Gardiner, J.I. Cirac and P.Zoller, Physical Review Letters Vol.75,3788 (1995).

27. Roland Omnès, The Interpretation of Quantum Mechanics, Princeton Series in Physics, (1994).

28. Wojciech H. Zurek Physics Today, October 1991 p.36.

29. D. Giulini, E. Joos, C. Kiefer, J. Kupsch, I.-O. Stamatescu, H.D. Zeh, Decoherence and the Appearance of a Classical World in Quantum Theory, Springer-Verlag, (1996).

30. A. Barchielli and V.P. Belavkin, Journal of Physics A 24, 1495 (1991).

31. Masahito Ueda, Physical Review A, Vol.41, 3875 (1990).

32. Masahito Ueda, Nobuyuki Imoto and Tetsuo Ogawa, Physical Review A, Vol.41, 3891 (1990).

33. Thomas Dean, James Allen, Yiannis Aloimonos, Artificial Intelligence, Theory and Practice, Addison-Wesley Publishing Company, (1995).

INITIAL DISTRIBUTION LIST

1. Defence Technical Information Center.....2
   8725 John J. Kingman RD.,STE 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library.....2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. Professor William Maier.....1
   Chairman, Department of Physics, Code PH/Mw
   Naval Postgraduate School
   Monterey, California 93943

4. Professor James Luscombe.....2
   Department of Physics, Code PH/Lj
   Naval Postgraduate School
   Monterey, California 93943

5. Professor Wolfgang Baer.....3
   Department of Computer Science Code CS
   Naval Postgraduate School
   Monterey, California 93943

6. CPT Dimitrios Giannakopoulos.....2
   20 Paparigopoulou Str.
   Athens, 11473
   Greece